Installatie-instructies voor Mac-Lab/ CardioLab Anti-Virus (NL)

Mac-Lab/CardioLab-softwareversie 6.9.6

Inleiding

Antivirussoftware is voor faciliteiten van grote waarde om te voldoen aan privacyvoorschriften, zoals HIPAA.

Gebruik van dit document

Gebruik dit document om gevalideerde antivirussoftware te installeren voor het Mac-Lab/ CardioLab v6.9.6-systeem.

Herziene uitgaven

Versie	Datum	Opmerkingen
A	16 februari 2016	Eerste publieke uitgave.
B	9 juni 2016	Update voor Trend Micro ter ondersteuning van CO_2.
C	16 mei 2017	Updates voor McAfee ePolicy Orchestrator, Trend Micro en Symantec.
D	10 juli 2017	Updates voor Symantec 12.1.6 MP5, Trend Micro 11.0 SP1, McAfee ePO 5.9 en McAfee VSE 8.8, patch 9.
E	14 augustus 2017	Verwijdering van verwijzingen naar McAfee ePolicy Orchestrator 5.9 en McAfee VirusScan Enterprise 8.8, patch 9. Toevoeging van gebruikersinterfacetalen aan 6.9.6 R3.
F	25 september 2017	McAfee ePO 5.9 en McAfee VSE 8.8, patch 9 toegevoegd. Koppelingen naar updates voor Trend Micro 11 en 12.

Aan de slag

Antivirusvereisten

WAARSCHUWING: INSTALLATIE VAN ANTIVIRUSSOFTWARE VEREIST

Het systeem wordt geleverd zonder antivirusbeveiliging. Zorg ervoor dat er een gevalideerd antivirusprogramma op het systeem wordt geïnstalleerd voordat u dit aansluit op een netwerk. Het ontbreken van een gevalideerde antivirusbeveiliging kan instabiliteit of een storing van het systeem tot gevolg hebben.

Houd rekening met de volgende vereisten:

- Antivirussoftware wordt niet meegeleverd met het Mac-Lab/CardioLab-systeem en het is de verantwoordelijkheid van de klant om deze software te verkrijgen, te installeren en te onderhouden.
- De klant is verantwoordelijk voor het bijwerken van virusdefinitiebestanden.
- Neem contact op met de systeembeheerder van de faciliteit en de technische ondersteuning van GE als een virus wordt aangetroffen.
- Installeer alleen de antivirussoftwarepakketten die zijn opgenomen in de lijst in de sectie Gevalideerde Antivirussoftware.
- Meld u aan als beheerder of lid van die groep om de in dit document beschreven activiteiten uit te voeren.
- Gebruik indien mogelijk een taalversie van de gevalideerde antivirussoftware die overeenkomt met de taal van het besturingssysteem. Als er geen gevalideerde antivirussoftware beschikbaar is in de taal van het besturingssysteem, installeert u de Engelse versie van de antivirussoftware.

Gevalideerde antivirussoftware

WAARSCHUWING: SYSTEEMINSTABILITEIT

Er mag geen niet-gevalideerde antivirussoftware (inclusief niet-gevalideerde versies) worden geïnstalleerd of gebruikt. Als dit toch wordt gedaan, kan het systeem instabiel worden of defect raken. Gebruik uitsluitend gevalideerde antivirussoftware in de juiste taalversie.

OPMERKING: Als de taalspecifieke antivirussoftware niet beschikbaar is, installeert u de Engelstalige versie van de antivirussoftware.

De Mac-Lab/CardioLab v6.9.6-systemen zijn gevalideerd voor gebruik met de in de volgende tabel vermelde software.

Ondersteunde antivirussoftware	Ondersteunde MLCL-talen	Ondersteunde versie van antivirussoftware
McAfee VirusScan Enterprise	Engels, Frans, Duits, Italiaans, Spaans, Zweeds, Noors, Deens, Nederlands, Chinees, Japans	8.8, patch 3 8.8, patch 4 8.8, patch 8 8.8, patch 9
McAfee ePolicy Orchestrator (met McAfee VirusScan Enterprise)	Engels, Frans, Duits, Italiaans, Spaans, Zweeds, Noors, Deens, Nederlands, Chinees, Japans	v5.0 v5.3.2 v5.9
Symantec EndPoint Protection	Engels, Frans, Duits, Italiaans, Spaans, Zweeds, Noors, Deens, Nederlands, Chinees, Japans	12.1.2, 12.1.6 MP5, 14.0 MP1
Trend Micro OfficeScan Client/Server Edition	Engels, Frans, Duits, Italiaans, Spaans, Zweeds, Noors, Deens, Nederlands, Chinees, Japans	10.6 SP2, 11.0 SP1, XG 12.0

De ondersteunde antivirussoftware is beschikbaar in de talen die zijn vermeld in de volgende tabel.

MLCL-versie	Ondersteunde MLCL-talen
M6.9.6 R1	Engels
M6.9.6 R2	Engels, Frans, Duits
M6.9.6 R3	Engels, Frans, Duits, Italiaans, Spaans, Zweeds, Noors, Deens, Nederlands, Chinees, Japans

Configuratie van de Anti-virus Management Console Server

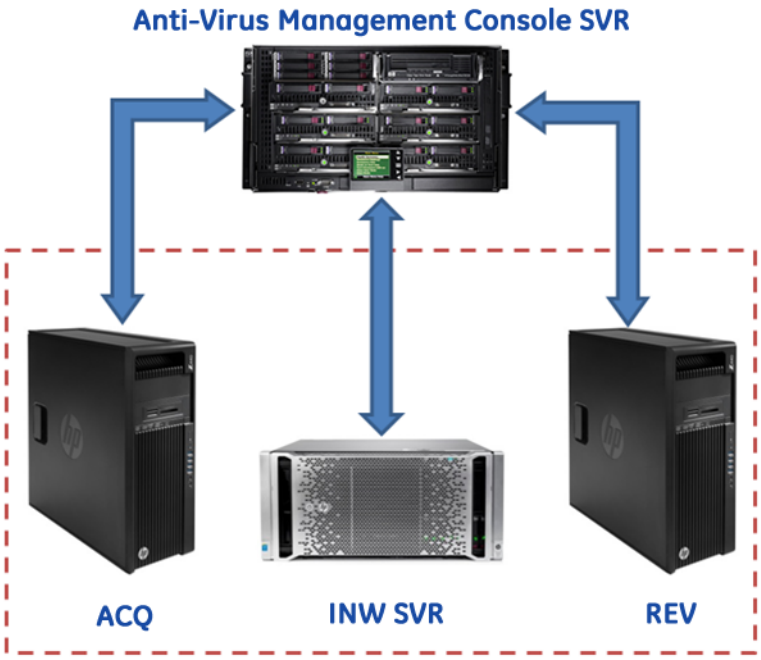
De Anti-virus Management Console moet worden geïnstalleerd op de Anti-Virus Management Console Server.

De communicatie tussen de Anti-virus Management Console Server en Mac-Lab/CardioLab-apparaten kan op verschillende manieren tot stand worden gebracht, afhankelijk van de omgeving:

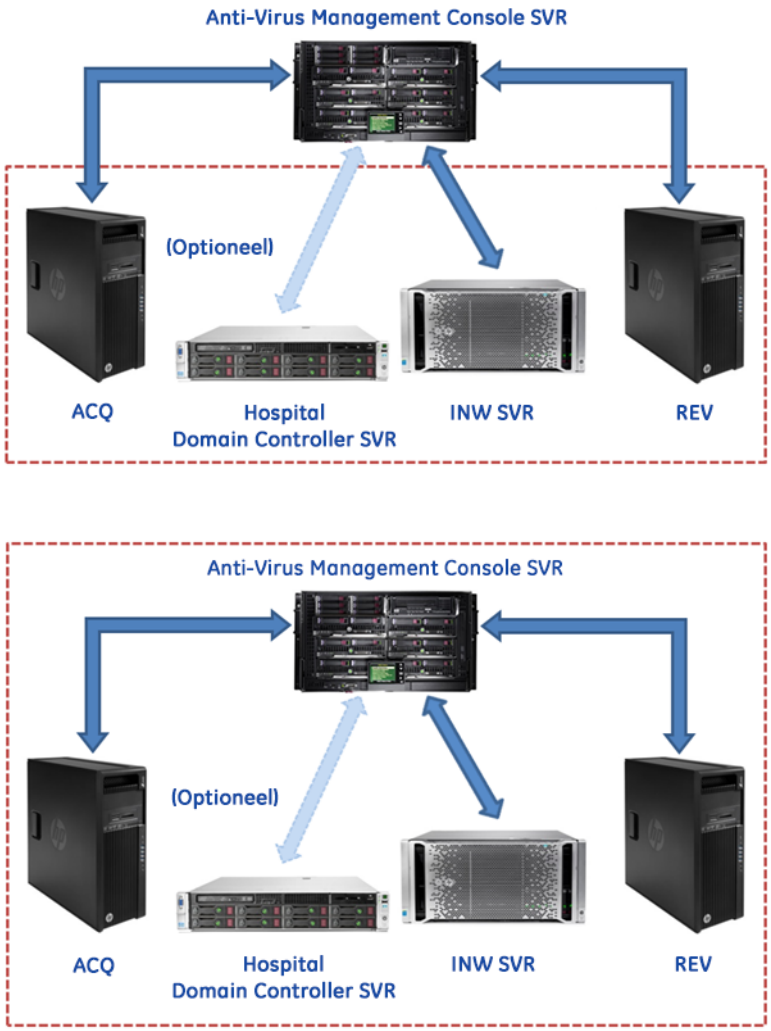
1. INW-domeincontrolleromgeving - Anti-virus Management Console SVR niet in het INW-serverdomein
   - Communicatietype - 1 <Zelfde netwerk met hetzelfde subnetmasker>
   - Communicatietype - 2 <Ander netwerk met ander subnetmasker>
2. Ziekenhuisdomeincontrolleromgeving - Anti-virus Management Console SVR niet in domein van de ziekenhuisdomeincontroller
   - Communicatietype - 1 <Ander netwerk met ander subnetmasker>
3. Ziekenhuisdomeincontrolleromgeving - Anti-virus Management Console SVR in domein van de ziekenhuisdomeincontroller
   - Communicatietype - 1 <Zelfde netwerk met hetzelfde subnetmasker>

OPMERKING: De Anti-virus Management Console Server moet twee netwerkpoorten hebben. Eén netwerkpoort moet worden verbonden met het Centricity Cardiology INW-netwerk en het tweede netwerkpoort moet worden verbonden met het ziekenhuisnetwerk.

Blokschema van de INW-domeincontrolleromgeving

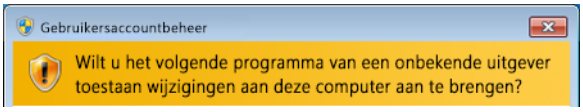


Blokschema van de ziekenhuisdomeincontrolleromgeving



Gebruikersaccountbeheer

Gebruikersaccountbeheer is een Windows-functie die onbevoegde wijzigingen op een computer voorkomt. Tijdens bepaalde procedures in deze handleiding wordt een melding van het Gebruikersaccountbeheer weergegeven.



Als deze melding wordt weergegeven als gevolg van het volgen van de procedures in deze handleiding, is het veilig om door te gaan.

Installatie-instructies voor antivirussoftware

Klik op de antivirussoftware die u wilt installeren:

Algemene installatieprocedures voor antivirussoftware

Gebruik de procedures in deze sectie wanneer daarnaar wordt verwezen in de installatie-instructies van de antivirussoftware.

Schakel de Loopback-verbinding uit

Schakel de Loopback-verbinding uit op een acquisitiesysteem dat is verbonden met de Mac-Lab/CardioLab-omgeving om alle clientsystemen met hetzelfde subnetmasker op het domein weer te geven.

1. Meld u aan als **Administrator** (Beheerder) of als lid van die groep.
2. Klik met de rechtermuisknop op het bureaublad op ***Network*** (Netwerk) en selecteer ***Properties*** (Eigenschappen).
3. Klik op ***Change adapter settings*** (Adapterinstellingen wijzigen).
4. Klik met de rechtermuisknop op ***Loopback Connection*** (Loopback-verbinding) en selecteer ***Disable*** (Uitschakelen).
5. Start het acquisitiesysteem opnieuw op.

OPMERKING: Het uitschakelen van de Loopback-verbinding op het acquisitiesysteem is vereist om alle clientsystemen met hetzelfde subnetmasker op het domein te ontdekken.

Schakel de Loopback-verbinding in

Schakel de Loopback-verbinding in op een acquisitiesysteem dat is verbonden met de Mac-Lab/CardioLab-omgeving door de onderstaande stappen te volgen.

1. Meld u aan als **Administrator** (Beheerder) of als lid van die groep.
2. Klik met de rechtermuisknop op het bureaublad op ***Network*** (Netwerk) en selecteer ***Properties*** (Eigenschappen).
3. Klik op ***Change adapter settings*** (Adapterinstellingen wijzigen).
4. Klik met de rechtermuisknop op ***Loopback Connection*** (Loopback-verbinding) en selecteer ***Enable*** (Inschakelen).
5. Start het acquisitiesysteem opnieuw op.

Configureer de Computerbrowserservice vóór installatie van de antivirussoftware

Controleer de Computerbrowserservice-instelling op aan een netwerk aangesloten acquisitie- en controlesystemen om er zeker van te zijn dat deze correct is geconfigureerd.

1. Klik op ***Start > Control Panel > Network and Sharing Center*** (Start > Configuratiescherm > Netwerkcentrum).
2. Klik op ***Change advanced sharing settings*** (Geavanceerde instellingen voor delen wijzigen).
3. Vouw ***Home or Work*** (Thuis of op het werk) uit.
4. Zorg ervoor dat ***Turn on file and printer sharing*** (Bestands- en printerdeling inschakelen) is geselecteerd.
5. Klik op ***Save changes*** (Wijzigingen opslaan).
6. Klik op ***Start > Run*** (Start > Uitvoeren).
7. Typ **services.msc** en druk op **Enter**.
8. Dubbelklik op de ***Computerbrowser***-service.
9. Zorg ervoor dat ***Startup type*** (Opstarttype) is ingesteld op ***Automatic*** (Automatisch). Als het niet op Automatic (Automatisch) is ingesteld, wijzig het dan en klik op ***Start***.
10. Klik op ***OK***.
11. Sluit het venster ***Services***.

Computerbrowserservice configureren na installatie van de antivirussoftware

Controleer na het installeren van de antivirussoftware de Computerbrowserservice-instelling op aan een netwerk aangesloten acquisitie- en controlesystemen om er zeker van te zijn dat deze correct is geconfigureerd.

1. Klik op ***Start > Run*** (Start > Uitvoeren).
2. Typ **services.msc** en druk op **Enter**.
3. Dubbelklik op de ***Computerbrowser***-service.
4. Verander ***Startup type*** (Opstarttype) naar ***Manual*** (Handmatig).
5. Klik op ***OK***.
6. Sluit het venster ***Services***.

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

Overzicht van de installatie

Installeer Symantec Endpoint Protection alleen in een Mac-Lab/CardioLab-netwerkomgeving. In een netwerkomgeving moet Symantec Endpoint Protection zijn geïnstalleerd op de Anti-virus Management Console Server en vervolgens worden geïmplementeerd op de Centricity Cardiology INW-server en het acquisitie/controlewerkstation als client. Gebruik de volgende instructies voor het installeren en configureren van ***Symantec Endpoint Protection***.

Virusupdates zijn de verantwoordelijkheid van de faciliteit. Zorg dat u de definities regelmatig bijwerkt, zodat de beveiliging van het systeem up-to-date is.

Voorbereiding van de installatie

1. De Symantec Anti-Virus Management Console moet worden geïnstalleerd volgens de instructies van Symantec en zal naar verwachting goed werken.
2. Meld u aan als **Administrator** (Beheerder) of als lid van die groep op alle clientsystemen (acquisitie, controle en INW-server) om de antivirussoftware te installeren.
3. Open de opdrachtprompt in de modus ***Run As Administrator*** (Als beheerder uitvoeren).
4. Ga naar C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

OPMERKING: Voor het configureren van de INW-server gaat u naar C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Typ **UpdateRegSymantec.ps1** en druk op ***Enter***.
6. Controleer of het script succesvol is uitgevoerd.

   Als het bovengenoemde pad niet aanwezig is, voert u de volgende stappen uit voor alle MLCL-systemen, behalve voor de MLCL 6.9.6R1 INW-server (serverbesturingssysteem: Windows Server 2008R2).

   a. Klik op ***Start*** en vervolgens op ***Run*** (Uitvoeren).

   b. Typ **Regedit.exe** en klik op ***OK***.

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

   d. Zoek het register ***State*** (Staat) en dubbelklik erop.

   e. Verander ***Base*** (Basis) naar ***Decimal*** (Decimaal).

   f. Verander ***Value data*** (Waardegegevens) in ***146432***.

   g. Klik op ***OK*** en sluit het register.

7. Schakel de Loopback-verbinding uit. Raadpleeg Schakel de Loopback-verbinding uit op pagina 6 voor meer informatie.

8. Configureer de Computerbrowserservice. Raadpleeg Configureer de Computerbrowserservice vóór installatie van de antivirussoftware op pagina 7 voor meer informatie.

Symantec EndPoint Protection - Nieuwe stappen voor implementatie van de installatie (de geprefereerde push-installatiemethode)

1. Klik op ***Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager***.
2. Voer de gebruikersnaam en het wachtwoord in om in te loggen op Symantec Endpoint Protection Manager. (Klik op ***Yes*** (Ja) als er een controlevraag verschijnt.)
3. Schakel ***Do not show this Welcome Page again*** (Deze welkomstpagina niet opnieuw weergeven) in en klik op ***Close*** (Sluiten) om het welkomstscherm te sluiten.

OPMERKING: In versie 14.0 MP1 klikt u op ***Close*** (Sluiten) om het scherm ***Getting Started on Symantec EndPoint Protection*** (Aan de slag met Symantec Endpoint Protection) te sluiten.

4. Klik op ***Admin*** (Beheerder) in het venster ***Symantec EndPoint Protection Manager***.
5. Klik op ***Install Packages*** (Pakketten installeren) in het onderste deelvenster.
6. Klik op ***Client Install Feature Set*** (Functieset voor clientinstallatie) in het bovenste deelvenster.
7. Klik met de rechtermuisknop op het venster ***Client Install Feature Set*** (Functieset voor clientinstallatie) en selecteer ***Add*** (Toevoegen). Het venster Add Client Install Feature Set (Functieset voor clientinstallatie toevoegen) wordt weergegeven.
8. Voer een passende naam in en sla deze op, want de set is later nog nodig.
9. Zorg ervoor dat de ***Feature set version*** (Versie van de functieset) ***12.1 RU2 of later is***.
10. Selecteer alleen de volgende functies en deselecteer de andere functies.
    - ***Virus, Spyware, and Basic Download Protection*** (Virus-, spyware- en eenvoudige downloadbeveiliging).
    - ***Advanced Download Protection*** (Geavanceerde downloadbeveiliging).
11. Klik op ***OK*** in het berichtvenster.
12. Alleen in de versies 12.1.2 en 12.1.6 MP5 klikt u op ***OK*** om het venster ***Add Client Install Feature Set*** (Functieset voor clientinstallatie toevoegen) te sluiten.
13. Klik op ***Home*** in het venster ***Symantec EndPoint Protection Manager***.
14. Volg één van de volgende instructies, afhankelijk van de softwareversie:
    - **Versie 12.1.2 en 12.1.6 MP5:** Selecteer ***Install protection client to computers*** (Installeer beveiligingsclient op computers) uit de vervolgkeuzelijst ***Common Tasks*** (Algemene taken) rechtsboven in het venster ***Home***. Het scherm Client Deployment Type (Type clientimplementatie) wordt weergegeven.
    - **Versie 14.0 MP1:** Klik op ***Clients*** in het venster ***Symantec EndPoint Protection Manager***. Klik op ***Install a client*** (Een client installeren) onder ***Tasks*** (Taken). Het scherm ***Client Deployment wizard*** (Clientimplementatiewizard) wordt weergegeven.

15. Selecteer ***New Package Deployment*** (Nieuwe pakketimplementatie) en klik op ***Next*** (Volgende).

16. Selecteer de naam van de functieset die is gemaakt in stap 8. Houd de andere instellingen als standaard en klik op ***Next*** (Volgende).

OPMERKING: In versie 14.1 MP1 schakelt u onder ***Scheduled Scans*** (Geplande scans) de selectievakjes ***Delay scheduled scans when running on batteries*** (Geplande scans uitstellen op batterijstroom) en ***Allow user-defined scheduled scans to run when scan author is not logged on*** (Door gebruiker gedefinieerde geplande scans toestaan wanneer de auteur van de scan niet is aangemeld) uit.

17. Selecteer ***Remote push*** (Externe push) en klik op ***Next*** (Volgende). Wacht totdat het scherm ***Computer selection*** (Computerselectie) wordt weergegeven.

18. Vouw ***<Domain>*** (Domein) uit (voorbeeld: INW). Systemen die verbonden zijn met het domein, worden weergegeven in het venster ***Computer selection*** (Computerselectie).

OPMERKING: Als niet alle systemen worden herkend, klikt u op ***Search Network*** (Zoek netwerk) en op ***Find Computers*** (Zoek Computers). Gebruik de detectiemethode ***Search by IP address*** (Zoeken op IP adres) voor het identificeren van de clientsystemen (acquisitie, controle en INW-server).

19. Selecteer alle Mac-Lab/CardioLab-clientapparaten die zijn verbonden met het domein en klik op **>>**. Het scherm ***Login Credentials*** (Aanmeldingsgegevens) wordt weergegeven.

20. Voer de gebruikersnaam, het wachtwoord en de domein/computernaam in en klik op ***OK***.

21. Zorg ervoor dat alle geselecteerde apparaten verschijnen onder ***Install Protection Client*** (Beveiligingsclient installeren) en klik op ***Next*** (Volgende).

22. Klik op ***Send*** (Verzenden) en wacht tot de Symantec-antivirussoftware is geïmplementeerd op alle clientsystemen (acquisitie-, controle- en INW-server). Na afloop verschijnt het scherm ***Deployment Summary*** (Implementatieoverzicht).

23. Klik op ***Next*** (Volgende) en vervolgens op ***Finish*** (Voltooien) om de Clientimplementatiewizard te voltooien.

24. Wacht tot het Symantec-pictogram verschijnt in het systeemvak en herstart alle clientapparaten (acquisitie, controle en INW-server). Meld u aan als Administrator (Beheerder) of als lid van die groep op alle clientapparaten na de herstart.

Symantec EndPoint Protection Manager Console-configuraties

1. Selecteer ***Start > All Programs > Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager***. Het aanmeldingsvenster van Symantec EndPoint Protection Manager wordt geopend.

2. Voer het wachtwoord voor de Symantec Endpoint Protection Manager Console in en klik op ***Log On*** (Aanmelden).

3. Selecteer het tabblad ***Policies*** (Beleid) en klik op ***Virus and Spyware Protection*** (Beveiliging tegen virussen en spyware) onder ***Policies*** (Beleid). Het venster ***Virus and Spyware Protection Policies*** (Antivirus- en antispywarebeleid) wordt geopend.

4. Klik op ***Add a Virus and Spyware Protection Policy*** (Voeg een antivirus- en antispywarebeleid toe) onder ***Tasks*** (Taken). Het venster ***Virus and Spyware Protection*** (Antivirus- en antispyware) wordt geopend.

5. Klik onder ***Windows Settings > Scheduled Scans*** (Windows-instellingen > Geplande scans) op ***Administrator-Defined Scans*** (Door beheerder gedefinieerde scans).

6. Selecteer ***Daily Scheduled Scan*** (Dagelijks geplande scan) en klik op ***Edit*** (Bewerken). Het venster ***Edit Scheduled Scan*** (Geplande scan bewerken) wordt geopend.

7. Wijzig de naam en de omschrijving van de scan naar respectievelijk ***Weekly Scheduled Scan*** (Wekelijks geplande scan) en ***Weekly Scan at 00:00*** (Wekelijkse scan om 00:00).

8. Selecteer ***Scan type*** (Scantype) als ***Full Scan*** (Volledige scan).

9. Selecteer het tabblad ***Schedule*** (Planning).

10. Selecteer onder ***Scanning Schedule*** (Scanplanning) de optie ***Weekly*** (Wekelijks) en verander de tijd naar ***00:00***.

11. Schakel onder ***Scan Duration*** (Scantijd) het selectievakje ***Randomize scan start time within this period (recommended in VMs)*** (Starttijd scan binnen deze periode willekeurig maken [aanbevolen voor VM's]) en selecteer ***Scan until finished (recommended to optimize scan performance)*** (Scan totdat voltooid [aanbevolen voor optimale scanprestaties]).

12. Schakel onder ***Missed scheduled Scans*** (Gemiste geplande scans) het selectievakje ***Retry the scan within*** (De scan opnieuw proberen binnen) uit.

13. Selecteer het tabblad ***Notifications*** (Meldingen).

14. Schakel het selectievakje ***Display a notification message on the infected computer*** (Geef een melding weer op de geïnfecteerde computer) uit en klik op ***OK***.

15. Selecteer het tabblad ***Advanced*** (Geavanceerd) in het venster ***Administrator-Defined Scans*** (Door beheerder gedefinieerde scans).

16. Schakel onder ***Scheduled Scans*** (Geplande scans) de selectievakjes ***Delay scheduled scans when running on batteries*** (Geplande scans uitstellen op batterijstroom), ***Allow user-defined scheduled scans to run when scan author is not logged on*** (Door gebruiker gedefinieerde geplande scans toestaan wanneer de auteur van de scan niet is aangemeld) en ***Display notifications about detections when the user logs on*** (Geef meldingen over detecties weer wanneer de gebruiker zich aanmeldt).

OPMERKING: In versie 14.0 MP1 schakelt u onder ***Scheduled Scans*** (Geplande scans) de selectievakjes ***Delay scheduled scans when running on batteries*** (Geplande scans uitstellen op batterijstroom) en ***Allow user-defined scheduled scans to run when scan author is not logged on*** (Door gebruiker gedefinieerde geplande scans toestaan wanneer de auteur van de scan niet is aangemeld) uit.

17. Schakel onder ***Startup and Triggered Scans*** (Opstarten en getriggerde scans) het selectievakje ***Run an Active Scan when new definitions arrive*** (Voer een actieve scan uit als nieuwe definities binnenkomen uit.

18. Klik onder ***Windows Settings (Windows-instellingen) > Protection Technology*** (Beveiligingstechnologie) op ***Auto-Protect*** (Automatische beveiliging).

19. Selecteer het tabblad ***Scan Details*** (Scangegevens) en selecteer en vergrendel ***Enable Auto-Protect*** (Auto-Protect inschakelen).

20. Selecteer het tabblad ***Notifications*** (Meldingen) en schakel de selectievakjes ***Display a notification message on the infected computer*** (Een meldingsbericht weergeven op de geïnfecteerde computer) en ***Display the Auto-Protect results dialog on infected computer*** (Dialoogvenster met Auto-Protect-resultaten weergeven op de geïnfecteerde computer) uit en vergrendel deze opties.

21. Selecteer het tabblad ***Advanced*** (Geavanceerd) en vergrendel onder ***Auto-Protect Reloading and Enablement*** (Herladen en inschakelen van Auto-Protect) de optie ***When Auto-Protect is disabled, Enable after:*** (Als Auto-Protect is uitgeschakeld, schakel in na:).

22. Klik onder ***Additional Options*** (Extra opties) op ***File Cache*** (Bestandscache). Het venster ***File Cache*** (Bestandscache) wordt geopend.

23. Schakel het selectievakje ***Rescan cache when new definitions load*** (Scan de cache opnieuw wanneer nieuwe definities worden geladen) uit en klik op ***OK***.

24. Klik onder ***Windows Settings > Protection Technology*** (Windows-instellingen > Beveiligingstechnologie) op ***Download Protection*** (Downloadbeveiliging).

25. Selecteer het tabblad ***Notifications*** (Meldingen) en schakel het selectievakje ***Display a notification message on the infected computer*** (Geef een melding weer op de geïnfecteerde computer) uit en vergrendel deze optie.

26. Klik onder ***Windows Settings > Protection Technology*** (Windows-instellingen > Beveiligingstechnologie) op ***SONAR***.

27. Selecteer het tabblad ***SONAR Settings*** (SONAR-instellingen) en schakel ***Enable SONAR*** (SONAR inschakelen) uit en vergrendel deze optie.

28. Klik onder ***Windows Settings > Protection Technology*** (Windows-instellingen > Beveiligingstechnologie) op ***Early Launch Anti-Malware Driver*** (Antimalwaredriver vroeg activeren).

29. Schakel het selectievakje ***Enable Symantec early launch anti-malware*** (Symantec-antimalwaredriver vroeg activeren inschakelen) uit en vergrendel deze optie.

30. Klik onder ***Windows Settings > Email Scans*** (Windows-instellingen > E-mailscans) op ***Internet Email Auto-Protect (Auto-Protect voor internet-e-mail)***.

31. Selecteer het tabblad ***Scan Details*** (Scangegevens) en schakel het selectievakje ***Enable Internet Email Auto-Protect*** (Auto-Protect voor internet-e-mail inschakelen) uit en vergrendel deze optie.

32. Selecteer het tabblad ***Notifications*** (Meldingen) en schakel de selectievakjes ***Display a notification message on the infected computer*** (Geef een melding weer op de geïnfecteerde computer), ***Display a progress indicator when email is being sent*** (Geef een voortgangsindicator weer wanneer e-mail wordt verzonden) en ***Display a notification area icon*** (Geef een pictogram weer in het meldingsgebied) uit en vergrendel deze opties.

33. Klik onder ***Windows Settings > Email Scans*** (Windows-instellingen > E-mailscans) op ***Microsoft Outlook Auto-Protect*** (Auto-Protect voor Microsoft Outlook).

34. Selecteer het tabblad ***Scan Details*** (Scangegevens) en schakel het selectievakje ***Enable Microsoft Outlook Auto-Protect*** (Auto-Protect voor Microsoft Outlook inschakelen) uit en vergrendel deze optie.

35. Selecteer het tabblad ***Notifications*** (Meldingen) en schakel het selectievakje ***Display a notification message on the infected computer*** (Geef een melding weer op de geïnfecteerde computer) uit en vergrendel deze optie.

36. Klik onder ***Windows Settings > Email Scans*** (Windows-instellingen > E-mailscans) op ***Lotus Notes Auto-Protect*** (Auto-Protect voor Lotus Notes).

37. Selecteer het tabblad ***Scan Details*** (Scangegevens) en schakel het selectievakje ***Enable Lotus Notes Auto-Protect*** (Auto-Protect voor Lotus Notes inschakelen) uit en vergrendel deze optie.

38. Selecteer het tabblad ***Notifications*** (Meldingen) en schakel het selectievakje ***Display a notification message on infected computer*** (Geef een melding weer op de geïnfecteerde computer) uit en vergrendel deze optie.

39. Klik onder ***Windows Settings > Advanced Options*** (Windows-instellingen > Geavanceerde opties) op ***Global Scan Options*** (Algemene scanopties).

40. Schakel onder ***Bloodhound(™) Detection Settings*** (Detectie-instellingen van Bloodhound(™)) het selectievakje ***Enable Bloodhound(™) heuristic virus detection*** (Heuristische virusdetectie van Bloodhound(™) inschakelen) uit en vergrendel deze optie.

41. Klik onder ***Windows Settings > Advanced Options*** (Windows-instellingen > Geavanceerde opties) op ***Quarantine (Quarantaine)***.

42. Selecteer het tabblad ***General*** (Algemeen) en selecteer ***Do nothing*** (Niets doen) onder ***When New Virus Definitions Arrive*** (Wanneer nieuwe virusdefinities binnenkomen).

43. Klik onder ***Windows Settings > Advanced Options*** (Windows-instellingen > Geavanceerde opties) op ***Miscellaneous*** (Diversen).

44. Selecteer het tabblad ***Notifications*** (Meldingen) en schakel de selectievakjes ***Display a notification message on the client computer when definitions are outdated*** (Bericht op de clientcomputer weergeven als definities zijn verouderd), ***Display a notification message on the client computer when Symantec Endpoint Protection is running without virus definitions*** (Melding weergeven als Symantec EndPoint Protection wordt uitgevoerd zonder virusdefinities) en ***Display Error messages with a URL to a solution*** (Foutberichten weergeven met een URL naar een oplossing) uit.

45. Klik op ***OK*** om het venster ***Virus and Spyware Protection Policy*** (Antivirus- en antispywarebeleid) te sluiten.

46. Klik op ***Yes*** (Ja) in het berichtvenster ***Assign Policies*** (Beleid toewijzen).

47. Selecteer ***My Company*** (Mijn bedrijf) en klik op ***Assign*** (Toewijzen).

48. Klik op ***Yes*** (Ja) in het berichtvenster.

49. Klik onder ***Policies*** (Beleid) op ***Firewall***.

50. Klik op ***Firewall policy*** (Firewallbeleid) onder ***Firewall Policies*** (Firewallbeleidsregels) en klik op ***Edit the policy*** (Het beleid bewerken) onder ***Tasks*** (Taken).

51. Selecteer het tabblad ***Policy Name*** (Beleidsnaam) en schakel het selectievakje ***Enable this policy*** (Dit beleid inschakelen) uit.

52. Klik op ***OK***.

53. Klik onder ***Policies*** (Beleid) op ***Intrusion Prevention*** (Indringingspreventie).

54. Klik op het beleid ***Intrusion Prevention*** (Indringingspreventie) onder ***Intrusion Prevention Policies*** (Indringingspreventiebeleid) en klik op ***Edit the policy*** (Het beleid bewerken) onder ***Tasks*** (Taken).
55. Selecteer het tabblad ***Policy Name*** (Beleidsnaam) en schakel het selectievakje ***Enable this policy*** (Dit beleid inschakelen) uit.
56. Volg één van de volgende instructies, afhankelijk van de softwareversie:
    - **Versie 12.1.2:** Klik op ***Settings*** (Instellingen) in het linker deelvenster.
    - **Versies 12.1.6 MP5 en 14.0 MP1:** Klik op ***Intrusion Prevention*** (Indringingspreventie) in het linker deelvenster.
57. Schakel de selectievakjes ***Enable Network Intrusion Prevention*** (Indringingspreventie op het netwerk inschakelen) en ***Enable Browser Intrusion Prevention for Windows*** (Indringingspreventie op de browser voor Windows inschakelen) uit en vergrendel deze opties.
58. Klik op ***OK***.
59. Klik onder ***Policies*** (Beleid) op ***Application and Device Control*** (Toepassings- en apparaatbesturing).
60. Klik op ***Application and Device Control Policy*** (Toepassings- en apparaatbesturingsbeleid) onder ***Application and Device Control Policies*** (Beleidsregels voor toepassings- en apparaatbesturing) en klik op ***Edit the policy*** (Het beleid bewerken) onder ***Tasks*** (Taken).
61. Selecteer het tabblad ***Policy Name*** (Beleidsnaam) en schakel het selectievakje ***Enable this policy*** (Dit beleid inschakelen) uit.
62. Klik op ***OK***.
63. Klik onder ***Policies*** (Beleid) op ***LiveUpdate***.
64. Selecteer ***LiveUpdate Settings policy*** (Beleid voor LiveUpdate-instellingen) en klik onder ***Tasks*** (Taken) op ***Edit the policy*** (Het beleid bewerken).
65. Klik onder ***Overview > Windows Settings*** (Overzicht > Windows-instellingen) op ***Server Settings*** (Serverinstellingen).
66. Zorg ervoor dat ***Use the default management server*** (Gebruik de standaard beheerserver) onder ***Internal or External LiveUpdate Server*** (Interne of externe LiveUpdate-server) is geselecteerd en schakel het selectievakje ***Use a LiveUpdate server*** (Gebruik een LiveUpdate-server uit.
67. Klik op ***OK***.
68. Klik onder ***Policies*** (Beleid) op ***Exceptions*** (Uitzonderingen).
69. Klik op ***Exceptions policy*** (Uitzonderingenbeleid) en klik onder ***Tasks*** (Taken) op ***Edit the policy*** (Het beleid bewerken).
70. Volg één van de volgende instructies, afhankelijk van de softwareversie:
    - **Versie 12.1.2 en 12.1.6 MP5:** Klik op ***Exceptions > Add > Windows Exceptions > Folder*** (Uitzonderingen > Toevoegen > Windows-uitzonderingen > Map).
    - **Versie 14.0 MP1:** Klik op de vervolgkeuzelijst ***Add*** (Toevoegen) en selecteer ***Windows Exceptions > Folder*** (Windows-uitzonderingen > Map).

71. Voer een voor een de paden **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL, D:\GEData\Studies**, **E:**, **G:** in en doe het volgende:

    a. Zorg ervoor dat ***Include subfolders*** (Inclusief submappen) is geselecteerd.

OPMERKING: Klik op ***Yes*** (Ja) als het berichtvenster ***Are you sure you want to exclude all subfolders from protection?*** (Weet u zeker dat u alle submappen wilt uitsluiten van beveiliging?) wordt weergegeven.

    b. Selecteer ***All*** (Alle) bij ***Specify the type of scan that excludes this folder*** (Geef het type scan op dat deze map uitsluit).

    c. In versie 14.0 MP1 klikt u op ***OK*** om de uitzondering toe te voegen.

72. Klik op ***OK***.

73. Klik op ***Assign the policy*** (Het beleid toewijzen) onder ***Tasks*** (Taken).

74. Selecteer ***My Company*** (Mijn bedrijf) en klik op ***Assign*** (Toewijzen).

75. Klik op ***Yes*** (Ja).

76. Klik op ***Clients*** in het linker deelvenster en selecteer het tabblad ***Policies*** (Beleid).

77. Selecteer ***Default Group*** (Standaardgroep) onder ***My Company*** (Mijn bedrijf) en schakel het selectievakje ***Inherit policies and settings from parent group "My Company"*** (Beleid en instellingen overnemen van de bovenliggende groep “Mijn bedrijf”) uit en klik op ***Communications Settings*** (Communicatie-instellingen) onder ***Location-Independent Policies and Settings*** (Locatieonafhankelijke beleidsregels en instellingen).

OPMERKING: Als een waarschuwingsmelding verschijnt, klik dan op ***OK*** en klik opnieuw op ***Communications Settings*** (Communicatie-instellingen) onder ***Location-Independent Policies and Settings*** (Locatieonafhankelijke beleidsregels en instellingen).

78. Zorg ervoor dat het selectievakje ***Download policies and content from the management server*** (Download beleidsregels en inhoud van de beheerserver) onder ***Download*** is ingeschakeld en dat ***Push mode*** (Push-modus) is geselecteerd.

79. Klik op ***OK***.

80. Klik op ***General Settings*** (Algemene instellingen) onder ***Location-independent Policies and Settings*** (Locatieonafhankelijk beleidsregels en instellingen).

81. Selecteer het tabblad ***Tamper Protection*** (Beveiliging tegen kwaadwillige wijzigingen) en schakel het selectievakje ***Protect Symantec security software from being tampered with or shut down*** (Beveiligingssoftware van Symantec beveiligen tegen kwaadwillige wijzigingen of uitschakeling) uit en vergrendel deze optie.

82. Klik op ***OK***.

83. Klik op ***Admin*** (Beheerder) en selecteer ***Servers***.

84. Onder ***Servers*** selecteert u ***Local Site (My Site)*** (Lokale site [Mijn site]).

85. Onder ***Tasks*** (Taken) selecteert u ***Edit Site Properties*** (Site-eigenschappen bewerken). Het venster ***Site Properties for Local Site (My Site)*** (Site-eigenschappen voor lokale site [Mijn site]) wordt geopend.

86. Selecteer het tabblad ***LiveUpdate*** en zorg ervoor dat de planning onder ***Download Schedule*** (Downloadplanning) is ingesteld op ***Every 4 hour(s)*** (Elke 4 uur).

87. Klik op ***OK***.

88. Klik op ***Log Off*** (Afmelden) en sluit de Symantec EndPoint Protection Manager Console. Zorg ervoor dat de beleidsregels van Symantec Endpoint Protection worden gepusht (verzonden) naar de clientsystemen.

Richtlijnen voor na de installatie van Symantec EndPoint Protection

1. Schakel de Loopback-verbinding in. Raadpleeg Schakel de Loopback-verbinding in op pagina 6 voor meer informatie.

2. Configureer de Computerbrowserservice. Raadpleeg Computerbrowserservice configureren na installatie van de antivirussoftware op pagina 7 voor meer informatie.

3. Open de opdrachtprompt in de modus ***Run As Administrator*** (Als beheerder uitvoeren).

4. Ga naar C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

OPMERKING: Voor het configureren van de INW-server gaat u naar C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Typ **RestoreRegSymantec.ps1** en druk op ***Enter***.

6. Controleer of het script succesvol is uitgevoerd.
   Let op: U moet controleren of het script **RestoreRegSymantec.ps1** goed is uitgevoerd voordat u verdergaat.

   Als het bovengenoemde pad niet aanwezig is, voert u de volgende stappen uit voor alle MLCL-systemen, behalve voor de MLCL 6.9.6R1 INW-server (serverbesturingssysteem: Windows Server 2008R2).

   a. Klik op ***Start*** en vervolgens op ***Run*** (Uitvoeren).

   b. Typ **Regedit.exe** en klik op ***OK***.

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

   d. Zoek het register ***State*** (Staat) en dubbelklik erop.

   e. Verander ***Base*** (Basis) naar ***Decimal*** (Decimaal).

   f. Wijzig de ***Value data*** (Waardegegevens) in ***65536***.

   g. Klik op ***OK*** en sluit het register.

McAfee VirusScan Enterprise

Overzicht van de installatie

McAfee VirusScan Enterprise moet worden geïnstalleerd op een afzonderlijk Mac-Lab/CardioLab-systeem en moet afzonderlijk worden beheerd. Gebruik de volgende instructies om McAfee VirusScan Enterprise te installeren en configureren.

Virusupdates zijn de verantwoordelijkheid van de faciliteit. Zorg dat u de definities regelmatig bijwerkt, zodat de beveiliging van het systeem up-to-date is.

Installatieprocedure van McAfee VirusScan Enterprise

1. Meld u aan als **Administrator** (Beheerder) of als lid van die groep.
2. Plaats de cd van **McAfee VirusScan Enterprise 8.8, patch 3**, **McAfee VirusScan Enterprise 8.8, patch 4**, **McAfee VirusScan Enterprise 8.8, patch 8** of **McAfee VirusScan Enterprise 8.8, patch 9** in het cd-station.
3. Dubbelklik op ***SetupVSE.Exe***. Het dialoogvenster van Windows Defender wordt weergegeven.
4. Klik op ***Yes*** (Ja). Het scherm McAfee VirusScan Enterprise Setup (Installatie) wordt weergegeven.
5. Klik op ***Next*** (Volgende). Het scherm McAfee End User License Agreement (Licentieovereenkomst) wordt weergegeven.
6. Lees de licentieovereenkomst en vul alle verplichte velden in. Klik op ***OK*** wanneer u klaar bent. Het scherm Select Setup Type (Type installatie selecteren) wordt weergegeven.
7. Selecteer ***Typical*** (Gebruikelijk) en klik op ***Next*** (Volgende). Het scherm Select Access Protection Level (Beveiligingsniveau voor toegang selecteren) wordt weergegeven.
8. Selecteer ***Standard Protection*** (Standaardbeveiliging) en klik op ***Next*** (Volgende). Het scherm Ready to Install (Gereed om te installeren) wordt weergegeven.
9. Klik op ***Install*** (Installeren) en wacht tot de installatie is voltooid. Na een geslaagde installatie van McAfee VirusScan Enterprise wordt het scherm ***McAfee Virus Scan Enterprise Setup has completed successfully*** (De installatie is voltooid) weergegeven.
10. Schakel het selectievakje ***Run On-Demand Scan*** (Scan op verzoek uitvoeren) uit en klik op ***Finish*** (Voltooien).
11. Als het venster ***Update in Progress*** (Update wordt uitgevoerd) wordt weergegeven, klikt u op ***Cancel*** (Annuleren).
12. Als er in een berichtvenster wordt gevraagd het systeem opnieuw op te starten, klikt u op ***OK***.
13. Start het systeem opnieuw op.
14. Meld u aan als **Administrator** (Beheerder) of als lid van die groep.

Configuratie van McAfee VirusScan Enterprise

1. Klik op ***Start > All Programs > McAfee > VirusScan Console***. Het scherm ***VirusScan Console*** wordt weergegeven.
2. Klik met de rechtermuisknop op ***Access Protection*** (Toegangsbeveiliging) en selecteer ***Properties*** (Eigenschappen). Het scherm ***Access Protection Properties*** (Eigenschappen voor toegangsbeveiliging) wordt weergegeven.
3. Klik op het tabblad ***Access Protection*** (Toegangsbeveiliging) en schakel de selectievakjes ***Enable access protection*** (Toegangsbeveiliging inschakelen) en ***Prevent McAfee services from being stopped*** (Voorkom dat McAfee-services worden gestopt) uit.
4. Klik op ***OK***.
5. Klik met de rechtermuisknop op ***Buffer Overflow Protection*** (Beveiliging tegen bufferoverloop) en selecteer ***Properties*** (Eigenschappen). Het venster ***Buffer Overflow Protection Properties*** (Eigenschappen voor beveiliging tegen bufferoverloop) wordt weergegeven.
6. Klik op het tabblad ***Buffer Overflow Protection*** (Beveiliging tegen bufferoverloop) en schakel het selectievakje ***Show the messages dialog box when a buffer overflow is detected*** (Berichtvenster weergeven wanneer een bufferoverloop wordt gedetecteerd) uit onder Buffer overflow settings (Instellingen voor bufferoverloop).
7. Schakel het selectievakje ***Enable buffer overflow protection*** (Beveiliging tegen bufferoverloop inschakelen) uit onder ***Buffer overflow settings*** (Instellingen voor bufferoverloop).
8. Klik op ***OK***.
9. Klik met de rechtermuisknop op ***On-Delivery Email Scanner*** (Directe e-mailscanner) en selecteer ***Properties*** (Eigenschappen). Het scherm ***On-Delivery Email Scanner Properties*** (Eigenschappen voor directe e-mailscanner) wordt weergegeven.
10. Klik op het tabblad ***Scan items*** (Scan-items) en schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown program threats and trojans*** (Zoek onbekende programmabedreigingen en trojans).
    - ***Find unknown macro threats*** (Zoek onbekende macrobedreigingen).
    - ***Find attachments with multiple extensions*** (Zoek bijlagen met meerdere extensies).
11. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
12. Selecteer ***Disabled*** (Uitgeschakeld) bij ***Sensitivity level*** (Gevoeligheidsniveau) onder ***Artemis (Heuristic network check for suspicious files)*** (Heuristische netwerkcontrole voor verdachte bestanden).
13. Klik op ***OK***.
14. Klik met de rechtermuisknop ***op On-Delivery Email Scanner*** (Directe e-mailscanner) en selecteer ***Disable*** (Uitschakelen).

15. Klik met de rechtermuisknop op ***On-Access Scanner*** (Scanner bij toegang) en selecteer ***Properties*** (Eigenschappen). Het scherm ***On-Access Scan Properties*** (Eigenschappen voor scannen bij toegang) wordt weergegeven.

16. Klik op het tabblad ***General*** (Algemeen) en selecteer ***Disabled*** (Uitgeschakeld) bij ***Sensitivity level*** (Gevoeligheidsniveau) onder ***Artemis (Heuristic network check for suspicious files)*** (Heuristische netwerkcontrole voor verdachte bestanden).

17. Klik op het tabblad ***ScriptScan*** en schakel het selectievakje ***Enable scanning of scripts*** (Scannen van scripts inschakelen) uit.

18. Klik op het tabblad ***Blocking*** (Blokkeren) en schakel het selectievakje ***Block the connection when a threat is detected in a shared folder*** (Blokkeer de verbinding wanneer een bedreiging wordt ontdekt in een gedeelde map) uit.

19. Klik op het tabblad ***Messages*** (Berichten) en schakel het selectievakje ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Het berichtvenster weergeven wanneer een virus wordt gedetecteerd en de specifieke tekst weergeven in het bericht) uit.

20. Klik op ***All Processes*** (Alle processen) in het linker deelvenster.

21. Klik op het tabblad ***Scan items*** (Scan-items) en schakel de volgende opties uit onder Heuristics (Heuristieken).

    - ***Find unknown unwanted programs and trojans*** (Zoek onbekende ongewenste programma's en trojans).
    - ***Find unknown macro threats*** (Zoek onbekende macrobedreigingen).

22. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).

23. Klik op het tabblad ***Exclusions*** (Uitsluitingen) en klik op ***Exclusions*** (Uitsluitingen). Het scherm ***Set Exclusions*** (Uitsluitingen instellen) wordt weergegeven.

24. Klik op ***Add*** (Toevoegen). Het scherm ***Add Exclusion Item*** (Uitsluitingsitem toevoegen) wordt weergegeven.

25. Selecteer ***By name/location*** (Op naam/locatie) en klik op ***Browse*** (Bladeren). Het scherm ***Browse for Files or Folders*** (Zoeken naar bestanden of mappen) wordt weergegeven.

26. Ga één voor één naar de mappen ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** en selecteer ***OK***.

27. Selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten) in het venster ***Add Exclusion Item*** (Uitzonderingsitem toevoegen) en klik op ***OK***.

28. Zorg ervoor dat de mappen C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies\, E:\, G:\ aanwezig zijn in het venster Set Exclusions (Uitsluitingen instellen).

29. Klik op ***OK***.

30. Klik met de rechtermuisknop op ***AutoUpdate*** (Automatisch bijwerken) en selecteer ***Properties*** (Eigenschappen). Het scherm McAfee AutoUpdate Properties – AutoUpdate (Eigenschappen voor McAfee AutoUpdate – AutoUpdate) wordt weergegeven.

31. Schakel de volgende opties uit onder ***Update Options*** (Opties voor bijwerken):

- ***Get new detection engine and data if available*** (Haal nieuwe detectie-engine en data op indien beschikbaar).
- ***Get other available updates (service packs, upgrades, etc.)*** (Haal andere beschikbare updates op [servicepakketten, upgrades, enz.]).

32. Klik op ***Schedule*** (Planning). Het scherm Schedule Settings (Instellingen voor planning) wordt weergegeven.
33. Schakel het selectievakje ***Enable (scheduled task runs at specified time)*** (Inschakelen [de geplande taak wordt op een opgegeven tijdstip uitgevoerd]) uit onder ***Schedule Settings*** (Instellingen voor planning).
34. Klik op ***OK***.
35. Klik op ***OK***.
36. Klik met de rechtermuisknop op het venster ***VirusScan Console*** en selecteer ***New On-Demand Scan Task*** (Nieuwe scanopdracht op verzoek).
37. Verander de naam van de nieuwe scan naar ***Weekly Scheduled Scan*** (Wekelijks geplande scan). Het scherm ***On-Demand Scan Properties - Weekly Scheduled Scan*** (Eigenschappen voor scanopdrachten op verzoek - Wekelijks geplande scan wordt weergegeven.
38. Klik op het tabblad ***Scan Items*** (Scan-items) en schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Options*** (Opties).
39. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown program threats*** (Zoek onbekende programmabedreigingen).
    - ***Find unknown macro threats*** (Zoek onbekende macrobedreigingen).
40. Klik op het tabblad ***Exclusions*** (Uitsluitingen) en klik op ***Exclusions*** (Uitsluitingen). Het scherm ***Set Exclusions*** (Uitsluitingen instellen) wordt weergegeven.
41. Klik op ***Add*** (Toevoegen). Het scherm ***Add Exclusion Item*** (Uitsluitingsitem toevoegen) wordt weergegeven.
42. Selecteer ***By name/location*** (Op naam/locatie) en klik op ***Browse*** (Bladeren). Het scherm ***Browse for Files or Folders*** (Zoeken naar bestanden of mappen) wordt weergegeven.
43. Ga één voor één naar de mappen ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** en selecteer ***OK***.
44. Selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten) in het venster ***Add Exclusion Item*** (Uitzonderingsitem toevoegen) en klik op ***OK***.
45. Zorg ervoor dat de mappen ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** aanwezig zijn in het venster ***Set Exclusions*** (Uitsluitingen instellen).
46. Klik op ***OK***.
47. Klik op het tabblad ***Performance*** (Prestaties) en selecteer ***Disabled*** (Uitgeschakeld) bij ***Sensitivity level*** (Gevoeligheidsniveau) onder ***Artemis (Heuristic network check for suspicious files)*** (Heuristische netwerkcontrole voor verdachte bestanden).
48. Klik op ***Schedule*** (Planning). Het scherm ***Schedule Settings*** (Instellingen voor planning) wordt weergegeven.

49. Klik op het tabblad ***Task*** (Taak) en selecteer ***Enable (scheduled task runs at specified time)*** (Inschakelen [de geplande taak wordt op een opgegeven tijdstip uitgevoerd]) onder ***Schedule Settings*** (Instellingen voor planning).
50. Klik op het tabblad ***Schedule*** (Planning) en selecteer het volgende:
    a. Run task (Taak uitvoeren): Weekly (Wekelijks).
    b. Start Time (Begintijd): 12:00 AM
    c. Every (Iedere): 1 Weeks, Sunday (1 week, zondag).
51. Klik op ***OK***.
52. Klik op ***OK***.
53. Klik op ***Tools > Alerts*** (Meldingen) in het venster ***VirusScan Console***. Het scherm Alert Properties (Eigenschappen van meldingen) wordt weergegeven.
54. Schakel de selectievakjes ***On-Access Scan*** (Scannen bij toegang),***On-Demand Scan and scheduled scans*** (Scannen op verzoek en volgens planning), ***Email Scan*** (E-mails scannen) en ***AutoUpdate*** uit.
55. Klik op ***Destination*** (Bestemming). Het scherm ***Alert Manager Client Configuration*** (Clientconfiguratie meldingsbeheer) wordt weergegeven.
56. Schakel het selectievakje ***Disable alerting*** (Meldingen uitschakelen) in.
57. Klik op ***OK***. Het scherm ***Alert Properties*** (Eigenschappen voor meldingen) wordt weergegeven.
58. Selecteer het tabblad ***Additional Alerting Options*** (Aanvullende meldingsopties).
59. Selecteer de optie ***Suppress all alerts (severities 0 to 4)*** (Alle meldingen uitschakelen [ernst 0 t/m 4]) in de vervolgkeuzelijst ***Severity Filter*** (Filter voor ernst).
60. Selecteer het tabblad ***Alert Manager Alerts*** (Meldingen meldingsbeheer).
61. Schakel het selectievakje ***Access Protection*** (Toegangsbeveiliging) uit.
62. Klik op ***OK*** om het venster ***Alert Properties*** (Eigenschappen voor meldingen) te sluiten.
63. Sluit het venster ***VirusScan Console***.

McAfee ePolicy Orchestrator

Overzicht van de installatie

Installeer McAfee ePolicy Orchestrator alleen in een Mac-Lab/CardioLab-netwerkomgeving. McAfee ePolicy Orchestrator moet worden geïnstalleerd op een Anti-virus Management Console Server en McAfee VirusScan Enterprise moet worden geïmplementeerd op de Centricity Cardiology INW-server en de acquisitie/controlewerkstations als client. Gebruik de volgende instructies om McAfee ePolicy Orchestrator te installeren en configureren.

Onderstaande instructies voor het pushen en configureren van McAfee VirusScan Enterprise gelden voor patch 3, patch 4, patch 8 en patch 9.

Virusupdates zijn de verantwoordelijkheid van de faciliteit. Zorg dat u de definities regelmatig bijwerkt, zodat de beveiliging van het systeem up-to-date is.

Voorbereiding van de installatie

1. McAfee Anti-Virus Management Console moet worden geïnstalleerd volgens de instructies van McAfee en zal naar verwachting goed werken.
2. Meld u aan als **Administrator** (Beheerder) of als lid van die groep op alle clientsystemen (acquisitie, controle en INW-server) om de antivirussoftware te installeren.
3. Schakel de Loopback-verbinding uit. Raadpleeg Schakel de Loopback-verbinding uit op pagina 6 voor meer informatie.
4. Neem voor de implementatie van McAfee VirusScan Enterprise 8.8, patch 9, contact op met McAfee om UTN-USERFirst-Object- en VeriSign Universal Root-certificaten alleen op INW-servers te installeren. Start het systeem opnieuw op zodra de certificaten zijn geïnstalleerd.

OPMERKING: Zonder de installatie van UTN-USERFirst-Object- en VeriSign Universal Root-certificaten kan McAfee VirusScan Enterprise 8.8, patch 9, niet worden geïnstalleerd op INW-servers.

5. Voeg voor nieuwe installaties de volgende agent-versie toe aan de hoofdopslagplaats van McAfee ePolicy Orchestrator in de McAfee ePolicy Orchestrator Console: ***- McAfee Agent v5.0.5.658***
6. Voeg voor nieuwe installaties het volgende pakket toe aan de hoofdopslagplaats van McAfee ePolicy Orchestrator in de 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).

OPMERKING: VSE880LMLRP3.zip bevat de installatiepakketten voor patch 2 en patch 3. Patch 2 is geschikt voor Windows 7 en het Windows Server 2008 OS-platform en patch 3 is geschikt voor Windows 8 en het Windows Server 2012 OS-platform. Het McAfee-installatieprogramma installeert de juiste patch door vast te stellen welk Windows-besturingssysteem wordt gebruikt.

7. Voeg voor nieuwe installaties de volgende extensies toe aan de extensietabel van McAfee ePolicy Orchestrator in de McAfee ePolicy Orchestrator Console:
   - McAfee VirusScan Enterprise 8.8, patch 3: VIRUSSCAN8800 v8.8.0.348 en VIRUSSCANREPORTS v1.2.0.228
   - McAfee VirusScan Enterprise 8.8, patch 4: VIRUSSCAN8800 v8.8.0.368 en VIRUSSCANREPORTS v1.2.0.236
   - McAfee VirusScan Enterprise 8.8, patch 8: VIRUSSCAN8800 v8.8.0.511 en VIRUSSCANREPORTS v1.2.0.311
   - McAfee VirusScan Enterprise 8.8, patch 9: VIRUSSCAN8800 v8.8.0.548 en VIRUSSCANREPORTS v1.2.0.346

OPMERKING: VIRUSSCAN8800(348).zip en VIRUSSCANREPORTS120(228).zip kunnen worden gevonden in het pakket McAfee VirusScan Enterprise 8.8, patch 3.

VIRUSSCAN8800(368).zip en VIRUSSCANREPORTS120(236).zip kunnen worden gevonden in het pakket McAfee VirusScan Enterprise 8.8, patch 4.

VIRUSSCAN8800(511).zip en VIRUSSCANREPORTS120(311).zip kunnen worden gevonden in het pakket McAfee VirusScan Enterprise 8.8, patch 8.

VIRUSSCAN8800(548).zip en VIRUSSCANREPORTS120(346).zip kunnen worden gevonden in het pakket McAfee VirusScan Enterprise 8.8, patch 9.

McAfee ePolicy Orchestrator 5.0 of 5.3.2 - Implementatiestappen voor nieuwe installaties (de geprefereerde push-installatiemethode)

1. Afhankelijk van de softwareversie selecteert u ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console (Openen)*** of ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console*** om u aan te melden bij de ePolicy Orchestrator Console.

OPMERKING: Klik op ***Continue with this website*** (Doorgaan met deze website) als het berichtvenster ***Security Alert*** (Beveiligingsmelding) wordt weergegeven.

2. Voer de gebruikersnaam en het wachtwoord in en klik op ***Log On*** (Aanmelden).
3. Selecteer ***Menu > System > System Tree*** (Menu > Systeem > Systeemstructuur). Het venster System Tree (Systeemstructuur) wordt geopend.
4. Klik op ***My Organization*** (Mijn organisatie) en klik met de focus op ***My Organization*** (Mijn organisatie) op ***System Tree Actions > New Systems*** (Acties in de systeemstructuur > Nieuwe systemen) in de linker benedenhoek van het scherm.
5. Selecteer ***Push agents and add systems to the current group (My Organization)*** (Verzend agents en voeg systemen toe aan de huidige groep [Mijn organisatie)]) en klik op ***Browse*** (Bladeren) bij Target systems (Doelsystemen).
6. Voer de gebruikersnaam en het wachtwoord van de **domain/local administrator** (domein/ lokale beheerder) in en klik op ***OK***.
7. Selecteer het ***INW***-domein uit de vervolgkeuzelijst ***Domain*** (Domein).
8. Selecteer de clientapparaten (acquisitie, controle en INW-server) die zijn verbonden met het domein en klik op ***OK***.

OPMERKING: Als de domeinnaam niet wordt vermeld in de vervolgkeuzelijst ***Domain*** (Domein), doe dan het volgende:

- Klik in het venster ***Browse for Systems*** (Systemen zoeken) op ***Cancel*** (Annuleren).
- Voer in het venster ***New Systems*** (Nieuwe systemen) de systeemnamen van de clientapparaten (acquisitie, controle en INW-server) handmatig in bij het veld ***Target systems*** (Doelsystemen) en ga door met de onderstaande stappen.

9. Selecteer ***Agent Version*** (Agent-versie) als ***McAfee Agent for Windows 4.8.0 (Current)*** (McAfee-agent voor Windows 4.8.0 [Huidig]) of ***McAfee Agent for Windows 5.0.4 (Current)*** (McAfee-agent voor Windows 5.0.4 [Huidig]). Voer de gebruikersnaam en het wachtwoord van de **domain administrator** (domeinbeheerder) in en klik op***OK***.

10. Controleer of de mappen correct zijn gemaakt in de clientapparaten (acquisitie, controle en INW-server), afhankelijk van de patchversie:

    - Controleer voor patches 3 en 4 of de map ***C:\Program Files\McAfee\Common Framework*** aanwezig is en of McAfee Agent is geïnstalleerd in dezelfde map.

    OPMERKING: Controleer voor de INW-server of de map ***C:\Program Files (x86)\McAfee\Common Framework*** aanwezig is en of McAfee Agent is geïnstalleerd in dezelfde map.

    - Controleer voor patch 8 of de map ***C:\Program Files\McAfee\Agent*** aanwezig is en of McAfee Agent is geïnstalleerd in dezelfde map.

    OPMERKING: Controleer voor de INW-server of de map ***C:\Program Files (x86)\McAfee\Common Framework*** aanwezig is.

11. Herstart de clientapparaten (acquisitie, controle en INW-server) en meld u aan als **domain administrator** (domeinbeheerder) of lid van die groep.

12. Afhankelijk van de softwareversie klikt u op ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** of ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console***.

13. Voer de gebruikersnaam en het wachtwoord in en klik op ***Log On*** (Aanmelden).

14. Klik op ***Menu > Systems > System Tree*** (Menu > Systemen > Systeemstructuur).

15. Klik op ***My Organization*** (Mijn organisatie) en klik met de focus op ***My Organization*** (Mijn organisatie) op het tabblad ***Assigned Client Tasks*** (Toegewezen clienttaken).

16. Klik op de knop ***Actions > New Client Task Assignment*** (Acties > Nieuwe clienttaaktoewijzing) onder aan het scherm. Het scherm Client Task Assignment Builder (Clienttaaktoewijzingsbouwer) wordt weergegeven.

17. Selecteer het volgende:

    a. **Product:** McAfee Agent

    b. **Task Type (Taaktype):** Product Deployment (Productimplementatie)

    c. **Task name (Taaknaam):** Create New Task (Nieuwe taak maken)

18. Vul de velden in het scherm ***Client Task Catalog*** (Clienttaakcatalogus): ***New Task (Nieuwe taak) - McAfee Agent: Product Deployment*** (Productimplementatie) als volgt in:

    a. **Task Name (Taaknaam):** Voer een passende naam voor de taak in

    b. **Target platforms (Doelplatformen):** Vensters

    c. **Products and components (Producten en onderdelen):** VirusScan Enterprise version which is qualified for v6.9.6 (VirusScan Enterprise-versie die geschikt is voor v6.9.6)

    d. **Options (Opties):** Run at every policy enforcement (Windows only) (Uitvoeren bij elke beleidshandhaving [alleen Windows]) als ***Options*** (Opties) beschikbaar is

19. Klik op ***Save*** (Opslaan).

20. Selecteer het volgende in het scherm ***1 Select Task*** (Taak selecteren):

    a. **Product:** McAfee Agent

b. **Task Type (Taaktype):** Product Deployment (Productimplementatie)

c. **Task Name (Taaknaam):** Newly created task name (Nieuw gemaakte taaknaam)

21. Klik op ***Next*** (Volgende). Het scherm 2 Schedule (Planning) wordt weergegeven.
22. Selecteer ***Run immediately*** (Onmiddellijk uitvoeren) uit de vervolgkeuzelijst ***Schedule type*** (Type planning).
23. Klik op ***Next*** (Volgende). Het scherm 3 Summary (Overzicht) wordt weergegeven.
24. Klik op ***Save*** (Opslaan). Het scherm ***System Tree*** (Systeemstructuur) wordt weergegeven.
25. Select het tabblad ***Systems*** (Systemen) en selecteer vervolgens alle clientapparaten (acquisitie-, controle- en INW-server) die verbonden zijn met het domein.
26. Klik op ***Wake up Agents*** (Agents activeren) onder in het venster.
27. Houd de standaardinstellingen en klik op ***OK***.
28. Wacht tot het McAfee-pictogram wordt weergegeven in het systeemvak en herstart alle clientapparaten (acquisitie, controle en INW-server) en meld u op alle clientapparaten aan als **Administrator** (beheerder) of lid van die groep.
29. Klik op de koppeling ***Log Off*** (Afmelden) om de McAfee ePolicy Orchestrator Console te sluiten.

McAfee ePolicy Orchestrator 5.9.0 - Implementatiestappen voor nieuwe installaties (geprefereerde push-installatiemethode)

1. Klik op ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Start > Alle programma's > McAfee > ePolicy Orchestrator > McAfee ePolicy Orchestrator 5.9.0 Console starten) om u aan te melden bij ePolicy Orchestrator Console.

OPMERKING: Klik op ***Continue with this website*** (Doorgaan met deze website) als het berichtvenster ***Security Alert*** (Beveiligingsmelding) wordt weergegeven.

2. Voer de gebruikersnaam en het wachtwoord in en klik op ***Log On*** (Aanmelden).
3. Selecteer ***Menu > System > System Tree*** (Menu > Systeem > Systeemstructuur). Het venster ***System Tree*** (Systeemstructuur) wordt geopend.
4. Klik op ***My Organization*** (Mijn organisatie). Houd het vergrootglas op ***My Organization*** (Mijn organisatie) en klik op ***New Systems*** (Nieuwe systemen) bovenin het scherm.
5. Selecteer ***Push agents and add systems to the current group (My Organization)*** (Verzend agents en voeg systemen toe aan de huidige groep [Mijn organisatie)]) en klik op ***Browse*** (Bladeren) bij Target systems (Doelsystemen).
6. Voer de gebruikersnaam en het wachtwoord van de **domain/local administrator** (domein/lokale beheerder) in en klik op ***OK***.
7. Selecteer het ***INW***-domein uit de vervolgkeuzelijst ***Domain*** (Domein).
8. Selecteer de clientapparaten (acquisitie, controle en INW-server) die zijn verbonden met het domein en klik op ***OK***.

OPMERKING: Als de domeinnaam niet wordt vermeld in de vervolgkeuzelijst ***Domain*** (Domein), doe dan het volgende:

- Klik in het venster ***Browse for Systems*** (Systemen zoeken) op ***Cancel*** (Annuleren).
- Voer in het venster ***New Systems*** (Nieuwe systemen) de systeemnamen van de clientapparaten (Acquisition, Review en INW Server) handmatig in, gescheiden door een komma in het veld ***Target systems*** (Doelsystemen) en ga door met de onderstaande stappen.

9. Selecteer ***McAfee Agent for Windows 5.0.5 (huidige versie)*** als ***Agent Version*** (Agent-versie). Voer de gebruikersnaam en het wachtwoord van de **domain administrator** (domeinbeheerder) in en klik op***OK***.
10. Controleer of de mapstructuur ***C:\Program Files\McAfee\Agent*** correct is gemaakt in de clientapparaten (Acquisition, Review en INW Server).
11. Herstart de clientapparaten (acquisitie, controle en INW-server) en meld u aan als **domain administrator** (domeinbeheerder) of lid van die groep.
12. Klik op ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Start > Alle programma's > McAfee > ePolicy Orchestrator > McAfee ePolicy Orchestrator 5.9.0 Console starten) om u aan te melden bij ePolicy Orchestrator Console.
13. Voer de gebruikersnaam en het wachtwoord in en klik op ***Log On*** (Aanmelden).
14. Klik op ***Menu > Systems > System Tree*** (Menu > Systemen > Systeemstructuur).
15. Klik op ***My Organization*** (Mijn organisatie) en klik met de focus op ***My Organization*** (Mijn organisatie) op het tabblad ***Assigned Client Tasks*** (Toegewezen clienttaken).
16. Klik op de knop ***Actions > New Client Task Assignment*** (Acties > Nieuwe clienttaaktoewijzing) onder aan het scherm. Het scherm ***Client Task Assignment Builder*** (Clienttaaktoewijzingsbouwer) wordt geopend.
17. Selecteer het volgende:
    a. **Product:** McAfee Agent
    b. **Task Type (Taaktype):** Product Deployment (Productimplementatie)
18. Klik op ***Task Actions > Create New Task*** (Taakacties > Nieuwe taak maken). Het scherm ***Create New Task*** (Nieuwe taak maken) wordt geopend.
19. Vul de velden in het scherm ***Create New Task*** (Nieuwe taak maken) op de volgende manier in:
    a. **Task Name (Taaknaam):** Voer een passende naam voor de taak in
    b. **Target platforms (Doelplatformen):** Windows (schakel alle andere opties uit)
    c. **Products and components (Producten en onderdelen):** VirusScan Enterprise 8.8.0,1804
20. Klik op ***Save*** (Opslaan). Het scherm ***Client Task Assignment Builder*** (Clienttaaktoewijzingsbouwer) wordt geopend.
21. Selecteer de volgende opties in het scherm ***Client Task Assignment Builder*** (Clienttaaktoewijzingsbouwer):
    a. **Product:** McAfee Agent

b. **Task Type (Taaktype):** Product Deployment (Productimplementatie)

c. **Task Name (Taaknaam):** Newly created task name (Nieuw gemaakte taaknaam)

d. **Type planning:** Direct uitvoeren

22. Klik op ***Save*** (Opslaan). Het scherm ***Assigned Client Tasks*** (Toegewezen clienttaken) wordt geopend.
23. Select het tabblad ***Systems*** (Systemen) en selecteer vervolgens alle clientapparaten (acquisitie-, controle- en INW-server) die verbonden zijn met het domein.
24. Klik op ***Wake up Agents*** (Agents activeren) onder in het venster.
25. Houd de standaardinstellingen en klik op ***OK***.
26. Wacht tot het McAfee-pictogram wordt weergegeven in het systeemvak en herstart alle clientapparaten (acquisitie, controle en INW-server) en meld u op alle clientapparaten aan als **Administrator** (beheerder) of lid van die groep.
27. Klik op de koppeling ***Log Off*** (Afmelden) om de McAfee ePolicy Orchestrator Console te sluiten.

Configuratie van McAfee ePolicy Orchestrator 5.0 en 5.3.2 Server Console

1. Afhankelijk van de softwareversie klikt u op ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** of ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console***.
2. Voer de gebruikersnaam en het wachtwoord in en klik op ***Log On*** (Aanmelden).
3. Klik op ***Menu > Systems > System Tree*** (Menu > Systemen > Systeemstructuur).
4. Klik op ***My Organization*** (Mijn organisatie) en klik met de focus op My Organization (Mijn organisatie) op het tabblad ***Assigned Client Tasks*** (Toegewezen clienttaken).
5. Klik op de knop ***Actions > New Client Task Assignment*** (Acties > Nieuwe clienttaaktoewijzing) onder aan het scherm. Het scherm ***Client Task Assignment Builder*** (Clienttaaktoewijzingsbouwer) wordt weergegeven.
6. Selecteer het volgende:

   a. ***Product:*** VirusScan Enterprise 8.8.0

   b. ***Task Type (Taaktype):*** On Demand Scan (Scannen op verzoek)

   c. ***Task name (Taaknaam):*** Create New Task (Nieuwe taak maken)

7. Vul de velden in het scherm ***Client Task Catalog*** (Clienttaakcatalogus): ***New Task (Nieuwe taak) - VirusScan Enterprise 8.8.0:*** Vul de velden in het scherm ***On Demand Scan*** (Scannen op verzoek) als volgt in:

   a. ***Task Name (Taaknaam):*** Weekly Scheduled Scan (Wekelijks geplande scan)

   b. ***Omschrijving:*** Weekly Scheduled Scan (Wekelijks geplande scan)

8. Klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
9. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Options*** (Opties).
10. Schakel de volgende opties uit onder Heuristics (Heuristieken):
    - ***Find unknown program threats (Zoek onbekende programmabedreigingen).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
11. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.
12. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.
13. Selecteer ***By pattern*** (Op patroon) en voer één voor één de mappen **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:** in en selecteer Also exclude subfolders (Submappen ook uitsluiten). Klik op ***OK***.
14. Klik op het tabblad ***Performance*** (Prestaties). Het scherm ***Performance*** (Prestaties) wordt weergegeven.
15. Selecteer ***Disabled*** (Uitgeschakeld) bij ***Artemis (Heuristic network check for suspicious files)*** (Heuristische netwerkcontrole voor verdachte bestanden).
16. Klik op ***Save*** (Opslaan).
17. Selecteer het volgende in het scherm ***1 Select Task*** (Taak selecteren):
    - ***Product:*** VirusScan Enterprise 8.8.0
    - ***Task Type (Taaktype):*** On Demand Scan (Scannen op verzoek)
    - ***Task Name (Taaknaam):*** Weekly Scheduled Scan (Wekelijks geplande scan)
18. Klik op ***Next*** (Volgende). Het scherm ***2 Schedule*** (Planning) wordt weergegeven.
19. Selecteer ***Weekly*** (Wekelijks) uit de vervolgkeuzelijst ***Schedule type*** (Type planning) en selecteer ***Sunday*** (Zondag).
20. Stel ***Start time*** (Starttijd) in op ***12:00 AM*** en selecteer ***Run Once at that time*** (Eenmaal uitvoeren op dat tijdstip).
21. Klik op ***Next*** (Volgende). Het scherm ***3 Summary*** (Overzicht) wordt weergegeven.
22. Klik op ***Save*** (Opslaan). Het scherm ***System Tree*** (Systeemstructuur) wordt weergegeven.
23. Selecteer het tabblad ***Assigned Policies*** (Toegewezen beleid). Het scherm ***Assigned Policies*** (Toegewezen beleid) wordt weergegeven.
24. Selecteer ***VirusScan Enterprise 8.8.0*** uit de vervolgkeuzelijst ***Product***.
25. Klik op ***My Default*** (Mijn standaardwaarde) bij ***On-Access General Policies*** (Algemeen beleid bij toegang). Het scherm ***VirusScan Enterprise 8.8.0 > On-Access General Policies > My Default*** (VirusScan Enterprise 8.8.0 > Algemeen beleid bij toegang > Mijn standaardwaarde) wordt weergegeven.

26. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor) en klik op het tabblad ***General*** (Algemeen). Het venster ***General*** (Algemeen) wordt weergegeven.
27. Selecteer ***Disabled*** (Uitgeschakeld) bij ***Artemis (Heuristic network check for suspicious files)*** (Heuristische netwerkcontrole voor verdachte bestanden).
28. Klik op het tabblad ***ScriptScan***. Het scherm ***ScriptScan*** wordt weergegeven.
29. Schakel het selectievakje ***Enable scanning of scripts*** (Scripts scannen inschakelen) uit.
30. Klik op het tabblad ***Blocking*** (Blokkeren). Het scherm ***Blocking*** (Blokkeren) wordt weergegeven.
31. Schakel het selectievakje ***Block the connection when a threatened file is detected in a shared folder*** (Blokkeer de verbinding wanneer een bedreiging wordt ontdekt in een gedeelde map) uit.
32. Klik op het tabblad ***Messages*** (Berichten). Het scherm ***Messages*** (Berichten) wordt weergegeven.
33. Schakel het selectievakje ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Berichtvenster weergeven wanneer een virus wordt gedetecteerd en de specifieke tekst weergeven in het bericht) uit.
34. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor) en klik op het tabblad ***General*** (Algemeen). Het scherm ***General*** (Algemeen) wordt weergegeven.
35. Selecteer ***Disabled*** (Uitgeschakeld) bij ***Artemis (Heuristic network check for suspicious files)*** (Heuristische netwerkcontrole voor verdachte bestanden).
36. Klik op het tabblad ***ScriptScan***. Het scherm ***ScriptScan*** wordt weergegeven.
37. Zorg ervoor dat het selectievakje ***Enable scanning of scripts*** (Scripts scannen inschakelen) is uitgeschakeld.
38. Klik op het tabblad ***Blocking*** (Blokkeren). Het scherm ***Blocking*** (Blokkeren) wordt weergegeven.
39. Schakel het selectievakje ***Block the connection when a threatened file is detected in a shared folder*** (Blokkeer de verbinding wanneer een bedreiging wordt ontdekt in een gedeelde map) uit.
40. Klik op het tabblad ***Messages*** (Berichten). Het scherm ***Messages*** (Berichten) wordt weergegeven.
41. Schakel het selectievakje ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Berichtvenster weergeven wanneer een virus wordt gedetecteerd en de specifieke tekst weergeven in het bericht) uit.
42. Klik op ***Save*** (Opslaan).
43. Klik op ***My Default*** (Mijn standaardwaarde) bij ***On-Access Default Processes Policies*** (Beleid voor standaardprocessen bij toegang). Het scherm ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Beleid voor standaardprocessen bij toegang > Mijn standaardwaarde) wordt geopend.
44. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).

45. Klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
46. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown unwanted programs and trojans (Zoek onbekende ongewenste programma's en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
47. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
48. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.
49. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.
50. Selecteer ***By pattern*** (Op patroon) en voer één voor één de mappen **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** in en selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten). Klik op ***OK***.
51. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor) en klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
52. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown unwanted programs and trojans (Zoek onbekende ongewenste programma's en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
53. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
54. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.
55. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.
56. Selecteer ***By pattern*** (Op patroon) en voer één voor één de mappen **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** in en selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten). Klik op ***OK***.
57. Klik op ***Save*** (Opslaan).
58. Klik op ***My Default*** (Mijn standaardwaarde) bij ***On-Access Low-Risk Processes Policies*** (Beleid voor processen met laag risico bij toegang). Het scherm ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies*** (Beleid voor processen met laag risico bij toegang) > My Default (Mijn standaardwaarde) wordt weergegeven.
59. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
60. Klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.

61. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown unwanted programs and trojans (Zoek onbekende ongewenste programma's en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
62. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
63. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.
64. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.
65. Selecteer ***By pattern*** (Op patroon) en voer één voor één de mappen **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** in en selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten). Klik op ***OK***.
66. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor) en klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
67. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown unwanted programs and trojans (Zoek onbekende ongewenste programma's en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
68. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
69. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.
70. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.
71. Selecteer ***By pattern*** (Op patroon) en voer één voor één de mappen **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** in en selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten). Klik op ***OK***.
72. Klik op ***Save*** (Opslaan).
73. Klik op ***My Default*** (Mijn standaardwaarde) bij ***On-Access High-Risk Processes Policies*** (Beleid voor processen met hoog risico bij toegang). Het scherm ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Beleid voor processen met hoog risico bij toegang > Mijn standaardwaarde) wordt weergegeven.
74. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
75. Klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
76. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):

- ***Find unknown unwanted programs and trojans (Zoek onbekende ongewenste programma's en trojans).***
- ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***

77. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
78. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.
79. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.
80. Selecteer ***By pattern*** (Op patroon) en voer één voor één de mappen **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** in en selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten). Klik op ***OK***.
81. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor) en klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
82. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown unwanted programs and trojans (Zoek onbekende ongewenste programma's en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
83. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
84. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.
85. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.
86. Selecteer By pattern (Op patroon) en voer één voor één de mappen **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** in en selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten). Klik op ***OK***.
87. Klik op ***Save*** (Opslaan).
88. Klik op ***My Default*** (Mijn standaardwaarde) bij ***On Delivery Email Scan Policies*** (Beleid voor direct e-mails scannen). Het scherm ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default*** (VirusScan Enterprise 8.8.0 > Beleid voor direct e-mails scannen > Mijn standaardwaarde) wordt weergegeven.
89. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
90. Klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
91. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken).
    - ***Find unknown program threats and trojans (Zoek onbekende programmabedreigingen en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***

- ***Find attachments with multiple extensions (Zoek bijlagen met meerdere extensies).***

92. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
93. Selecteer ***Disabled*** (Uitgeschakeld) bij ***Artemis (Heuristic network check for suspicious files)*** (Heuristische netwerkcontrole voor verdachte bestanden).
94. Schakel het selectievakje ***Enable on-delivery email scanning*** (Direct e-mails scannen inschakelen) uit onder ***Scanning of email*** (E-mails scannen).
95. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
96. Klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
97. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown program threats and trojans (Zoek onbekende programmabedreigingen en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
    - ***Find attachments with multiple extensions (Zoek bijlagen met meerdere extensies).***
98. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
99. Selecteer ***Disabled*** (Uitgeschakeld) bij ***Artemis (Heuristic network check for suspicious files)*** (Heuristische netwerkcontrole voor verdachte bestanden).
100. Schakel het selectievakje ***Enable on-delivery email scanning*** (Direct e-mails scannen inschakelen) uit onder ***Scanning of email*** (E-mails scannen).
101. Klik op ***Save*** (Opslaan).
102. Klik op ***My Default*** (Mijn standaardwaarde) bij ***General Options Policies*** (Beleid voor algemene opties). Het scherm ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** (VirusScan Enterprise 8.8.0 > Beleid voor algemene opties > Mijn standaardwaarde) wordt weergegeven.
103. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
104. Klik op het tabblad ***Display Options*** (Weergaveopties). Het scherm ***Display Options*** (Weergaveopties) wordt weergegeven.
105. Selecteer het volgende onder ***Console options*** (Consoleopties):
    - ***Display managed tasks in the client console (Geef beheerde taken in de clientconsole weer).***
    - ***Disable default AutoUpdate task schedule (Schakel de standaard takenplanning van AutoUpdate uit).***
106. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
107. Klik op het tabblad ***Display Options*** (Weergaveopties). Het scherm ***Display Options*** (Weergaveopties) wordt weergegeven.
108. Selecteer het volgende onder ***Console options*** (Consoleopties).

- ***Display managed tasks in the client console (Geef beheerde taken in de clientconsole weer).***
- ***Disable default AutoUpdate task schedule (Schakel de standaard takenplanning van AutoUpdate uit).***

109. Klik op ***Save*** (Opslaan).
110. Klik op ***My Default*** (Mijn standaardwaarde) bij ***Alert Policies*** (Meldingenbeleid). Het scherm ***VirusScan Enterprise 8.8.0 > Alert Policies > My Default*** (VirusScan Enterprise 8.8.0 > Meldingenbeleid > Mijn standaardwaarde) wordt weergegeven.
111. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
112. Klik op het tabblad ***Alert Manager Alerts*** (Meldingen meldingsbeheer). Het scherm ***Alert Manager Alerts*** (Meldingen meldingsbeheer) wordt weergegeven.
113. Schakel de selectievakjes ***On-Access Scan*** (Scannen bij toegang), ***On-Demand Scan and scheduled scans*** (Scannen op verzoek en volgens schema), ***Email Scan*** (E-mails scannen) en ***AutoUpdate*** uit onder Components that generate alerts (Onderdelen die meldingen genereren).
114. Selecteer ***Disable alerting*** (Meldingen uitschakelen) onder de opties voor ***Alert Manager*** (Meldingsbeheer).
115. Schakel het selectievakje ***Access Protection*** (Toegangsbeveiliging) uit onder ***Components that generate alerts*** (Onderdelen die meldingen genereren).
116. Klik op ***Additional Alerting Options*** (Aanvullende meldingsopties). Het scherm ***Additional Alerting Options*** (Aanvullende meldingsopties) wordt weergegeven.
117. Selecteer uit het vervolgkeuzemenu ***Severity Filters*** (Filters voor ernst) ***Suppress all alerts (severities 0 to 4)*** (Alle meldingen uitschakelen [ernst 0 t/m 4]).
118. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor) en selecteer het tabblad ***Alert Manager Alerts*** (Meldingen meldingsbeheer). Het scherm ***Alert Manager Alerts*** (Meldingen meldingsbeheer) wordt weergegeven.
119. Schakel de selectievakjes ***On-Access Scan*** (Scannen bij toegang), ***On-Demand Scan and scheduled scans*** (Scannen op verzoek en volgens schema), ***Email Scan*** (E-mails scannen) en ***AutoUpdate*** uit onder Components that generate alerts Onderdelen (die meldingen genereren).
120. Schakel het selectievakje ***Disable alerting*** (Meldingen uitschakelen) in onder de opties voor ***Alert Manager*** (Meldingsbeheer).
121. Schakel het selectievakje ***Access Protection*** (Toegangsbeveiliging) uit onder ***Components that generate alerts*** (Onderdelen die meldingen genereren).
122. Klik op ***Additional Alerting Options*** (Aanvullende meldingsopties). Het scherm Additional Alerting Options (Aanvullende meldingsopties) wordt weergegeven.
123. Selecteer uit het vervolgkeuzemenu ***Severity Filters*** (Filters voor ernst) ***Suppress all alerts (severities 0 to 4)*** (Alle meldingen uitschakelen [ernst 0 t/m 4]).
124. Klik op ***Save*** (Opslaan).
125. Klik op ***My Default*** (Mijn standaardwaarde) bij ***Access Protection Policies*** (Beleid voor toegangsbeveiliging). Het scherm ***VirusScan Enterprise 8.8.0 > Access Protection***

Policies > My Default (VirusScan Enterprise 8.8.0 > Beleid voor toegangsbeveiliging > Mijn standaardwaarde) wordt weergegeven.

126. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
127. Klik op het tabblad ***Access Protection*** (Toegangsbeveiliging). Het scherm ***Access Protection*** (Toegangsbeveiliging) wordt weergegeven.
128. Schakel de volgende opties uit onder ***Access protection settings*** (Instellingen voor toegangsbeveiliging):
    - ***Enable access protection (Toegangsbeveiliging inschakelen).***
    - ***Prevent McAfee services from being stopped (Voorkomen dat McAfee-services worden gestopt).***
129. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
130. Klik op het tabblad ***Access Protection*** (Toegangsbeveiliging). Het scherm ***Access Protection*** (Toegangsbeveiliging) wordt weergegeven.
131. Schakel de volgende opties uit onder ***Access protection settings*** (Instellingen voor toegangsbeveiliging):
    - ***Enable access protection (Toegangsbeveiliging inschakelen).***
    - ***Prevent McAfee services from being stopped (Voorkomen dat McAfee-services worden gestopt).***
132. Klik op ***Save*** (Opslaan).
133. Selecteer ***My Default*** (Mijn standaardwaarde) bij ***Buffer Overflow Protection Policies*** (Beleid voor beveiliging tegen bufferoverloop). Het scherm ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Beleid voor beveiliging tegen bufferoverloop > Mijn standaardwaarde) wordt weergegeven.
134. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
135. Klik op het tabblad ***Buffer Overflow Protection*** (Beveiliging tegen bufferoverloop). Het scherm ***Buffer Overflow Protection*** (Beveiliging tegen bufferoverloop) wordt weergegeven.
136. Schakel het selectievakje ***Show the messages dialog when a buffer overflow is detected*** (Berichtvenster tonen wanneer een bufferoverloop wordt gedetecteerd) uit onder ***Client system warning*** (Clientsysteemwaarschuwing).
137. Schakel het selectievakje ***Enable buffer overflow protection*** (Beveiliging tegen bufferoverloop inschakelen) uit onder ***Buffer overflow settings*** (Instellingen voor bufferoverloop).
138. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
139. Klik op het tabblad ***Buffer Overflow Protection*** (Beveiliging tegen bufferoverloop). Het scherm ***Buffer Overflow Protection*** (Beveiliging tegen bufferoverloop) wordt weergegeven.
140. Schakel het selectievakje ***Show the messages dialog when a buffer overflow is detected*** (Berichtvenster tonen wanneer een bufferoverloop wordt gedetecteerd) uit onder ***Client system warning*** (Clientsysteemwaarschuwing).

141. Schakel het selectievakje ***Enable buffer overflow protection*** (Beveiliging tegen bufferoverloop inschakelen) uit onder ***Buffer overflow settings*** (Instellingen voor bufferoverloop).

142. Klik op ***Save*** (Opslaan).

143. Selecteer ***McAfee Agent*** uit het vervolgkeuzemenu ***Product***. Het venster ***Policies*** (Beleid) voor McAfee Agent wordt weergegeven.

144. Klik op ***My Default*** (Mijn standaardwaarde) bij ***Repository*** (Opslagplaats). Het scherm ***McAfee Agent > Repository > My Default*** (McAfee Agent > Opslagplaats > Mijn standaardwaarde) wordt weergegeven.

145. Klik op het tabblad ***Proxy***. Het scherm ***Proxy*** wordt weergegeven.

146. Selecteer ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** (Gebruik Internet Explorer-instellingen [voor Windows]/Instellingen voor systeemvoorkeuren [voor Mac OSX]) onder ***Proxy settings*** (Proxy-instellingen).

147. Klik op ***Save*** (Opslaan).

148. Klik op het tabblad ***Systems*** (Systemen).

149. Selecteer alle clientsystemen (acquisitie, controle en Centricity Cardiology INW-server) waarin u het geconfigureerde beleid wilt implementeren.

150. Selecteer ***Wake Up Agents*** (Agents activeren). Het scherm ***Wake Up Agent*** (Agent activeren) wordt weergegeven.

151. Klik op ***OK***.

152. Meld de ePolicy Orchestrator af.

Serverconfiguratie McAfee ePolicy Orchestrator 5.9.0 Console

1. Klik afhankelijk van de softwareversie op ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** (Start > Alle programma's > McAfee > ePolicy Orchestrator > McAfee ePolicy Orchestrator 5.9.0 Console starten).

2. Voer de gebruikersnaam en het wachtwoord in en klik op ***Log On*** (Aanmelden).

3. Klik op ***Menu > Systems > System Tree*** (Menu > Systemen > Systeemstructuur).

4. Klik op ***My Organization*** (Mijn organisatie) en klik met de focus op My Organization (Mijn organisatie) op het tabblad ***Assigned Client Tasks*** (Toegewezen clienttaken).

5. Klik op de knop ***Actions > New Client Task Assignment*** (Acties > Nieuwe clienttaaktoewijzing) onder aan het scherm. Het scherm ***Client Task Assignment Builder*** (Clienttaaktoewijzingsbouwer) wordt weergegeven.

6. Selecteer het volgende:

    a. ***Product:*** VirusScan Enterprise 8.8.0

    b. ***Task Type (Taaktype):*** On Demand Scan (Scannen op verzoek)

7. Klik in ***Task Actions*** (Taakacties) op ***Create New Task*** (Nieuwe taak maken). Het scherm ***Create New Task*** (Nieuwe taak maken) wordt geopend.

8. Vul de velden in het scherm ***Create New Task*** (Nieuwe taak maken) op de volgende manier in:

    a. ***Task Name (Taaknaam):*** Weekly Scheduled Scan (Wekelijks geplande scan)

    b. ***Omschrijving:*** Weekly Scheduled Scan (Wekelijks geplande scan)

9. Klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.

10. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Options*** (Opties).

11. Schakel de volgende opties uit onder Heuristics (Heuristieken):

    - ***Find unknown program threats (Zoek onbekende programmabedreigingen).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***

12. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.

13. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.

14. Selecteer ***By pattern*** (Op patroon) en voer één voor één de mappen **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:** in en selecteer Also exclude subfolders (Submappen ook uitsluiten). Klik op ***OK***.

15. Klik op het tabblad ***Performance*** (Prestaties). Het scherm ***Performance*** (Prestaties) wordt geopend.

16. Selecteer ***Disabled*** (Uitgeschakeld) bij ***Artemis (Heuristic network check for suspicious files)*** (Heuristische netwerkcontrole voor verdachte bestanden).

17. Klik op ***Save*** (Opslaan). Het scherm ***Client Task Assignment Builder*** (Clienttaaktoewijzingsbouwer) wordt geopend.

18. Selecteer de volgende opties in het scherm Client Task Assignment Builder (Clienttaaktoewijzingsbouwer):

    - ***Product:*** VirusScan Enterprise 8.8.0
    - ***Task Type (Taaktype):*** On Demand Scan (Scannen op verzoek)
    - ***Task Name (Taaknaam):*** Weekly Scheduled Scan (Wekelijks geplande scan)

19. Selecteer ***Weekly*** (Wekelijks) uit de vervolgkeuzelijst ***Schedule type*** (Type planning) en selecteer ***Sunday*** (Zondag).

20. Stel ***Start time*** (Starttijd) in op ***12:00 AM*** en selecteer ***Run Once at that time*** (Eenmaal uitvoeren op dat tijdstip).

21. Klik op ***Save*** (Opslaan). Het scherm ***Assigned Client Tasks*** (Toegewezen clienttaken) wordt geopend.

22. Selecteer het tabblad ***Assigned Policies*** (Toegewezen beleid). Het scherm ***Assigned Policies*** (Toegewezen beleid) wordt weergegeven.

23. Selecteer ***VirusScan Enterprise 8.8.0*** uit de vervolgkeuzelijst ***Product***.

24. Klik op ***My Default*** (Mijn standaardwaarde) bij ***On-Access General Policies*** (Algemeen beleid bij toegang). Het scherm ***VirusScan Enterprise 8.8.0 > On-Access General Policies > My***

Default (VirusScan Enterprise 8.8.0 > Algemeen beleid bij toegang > Mijn standaardwaarde) wordt weergegeven.

25. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor) en klik op het tabblad ***General*** (Algemeen). Het venster ***General*** (Algemeen) wordt weergegeven.
26. Selecteer ***Disabled*** (Uitgeschakeld) bij ***Artemis (Heuristic network check for suspicious files)*** (Heuristische netwerkcontrole voor verdachte bestanden).
27. Klik op het tabblad ***ScriptScan***. Het scherm ***ScriptScan*** wordt weergegeven.
28. Schakel het selectievakje ***Enable scanning of scripts*** (Scripts scannen inschakelen) uit.
29. Klik op het tabblad ***Blocking*** (Blokkeren). Het scherm ***Blocking*** (Blokkeren) wordt weergegeven.
30. Schakel het selectievakje ***Block the connection when a threatened file is detected in a shared folder*** (Blokkeer de verbinding wanneer een bedreiging wordt ontdekt in een gedeelde map) uit.
31. Klik op het tabblad ***Messages*** (Berichten). Het scherm ***Messages*** (Berichten) wordt weergegeven.
32. Schakel het selectievakje ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Berichtvenster weergeven wanneer een virus wordt gedetecteerd en de specifieke tekst weergeven in het bericht) uit.
33. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor) en klik op het tabblad ***General*** (Algemeen). Het venster ***General*** (Algemeen) wordt weergegeven.
34. Selecteer ***Disabled*** (Uitgeschakeld) bij ***Artemis (Heuristic network check for suspicious files)*** (Heuristische netwerkcontrole voor verdachte bestanden).
35. Klik op het tabblad ***ScriptScan***. Het scherm ***ScriptScan*** wordt weergegeven.
36. Zorg ervoor dat het selectievakje ***Enable scanning of scripts*** (Scripts scannen inschakelen) is uitgeschakeld.
37. Klik op het tabblad ***Blocking*** (Blokkeren). Het scherm ***Blocking*** (Blokkeren) wordt weergegeven.
38. Schakel het selectievakje ***Block the connection when a threatened file is detected in a shared folder*** (Blokkeer de verbinding wanneer een bedreiging wordt ontdekt in een gedeelde map) uit.
39. Klik op het tabblad ***Messages*** (Berichten). Het scherm ***Messages*** (Berichten) wordt weergegeven.
40. Schakel het selectievakje ***Show the messages dialog box when a threat is detected and display the specified text in the message*** (Berichtvenster weergeven wanneer een virus wordt gedetecteerd en de specifieke tekst weergeven in het bericht) uit.
41. Klik op ***Save*** (Opslaan). Het scherm Assigned Policies (Toegewezen beleid) wordt weergegeven.
42. Klik op ***My Default*** (Mijn standaardwaarde) bij ***On-Access Default Processes Policies*** (Beleid voor standaardprocessen bij toegang). Het scherm ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Beleid voor standaardprocessen bij toegang > Mijn standaardwaarde) wordt geopend.

43. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
44. Klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
45. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown unwanted programs and trojans (Zoek onbekende ongewenste programma's en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
46. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
47. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.
48. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.
49. Selecteer ***By pattern*** (Op patroon) en voer één voor één de mappen **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** in en selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten). Klik op ***OK***.
50. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor) en klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
51. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown unwanted programs and trojans (Zoek onbekende ongewenste programma's en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
52. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
53. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.
54. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.
55. Selecteer ***By pattern*** (Op patroon) en voer één voor één de mappen **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** in en selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten). Klik op ***OK***.
56. Klik op ***Save*** (Opslaan). Het scherm ***Assigned Policies*** (Toegewezen beleid) wordt weergegeven.
57. Klik op ***My Default*** (Mijn standaardwaarde) bij ***On-Access Low-Risk Processes Policies*** (Beleid voor processen met laag risico bij toegang). Het scherm ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies*** (Beleid voor processen met laag risico bij toegang) > My Default (Mijn standaardwaarde) wordt weergegeven.
58. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
59. Klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.

60. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown unwanted programs and trojans (Zoek onbekende ongewenste programma's en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
61. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
62. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.
63. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.
64. Selecteer ***By pattern*** (Op patroon) en voer één voor één de mappen **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** in en selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten). Klik op ***OK***.
65. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor) en klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
66. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown unwanted programs and trojans (Zoek onbekende ongewenste programma's en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
67. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
68. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.
69. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.
70. Selecteer ***By pattern*** (Op patroon) en voer één voor één de mappen **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** in en selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten). Klik op ***OK***.
71. Klik op ***Save*** (Opslaan). Het scherm ***Assigned Policies*** (Toegewezen beleid) wordt weergegeven.
72. Klik op ***My Default*** (Mijn standaardwaarde) bij ***On-Access High-Risk Processes Policies*** (Beleid voor processen met hoog risico bij toegang). Het scherm ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** (VirusScan Enterprise 8.8.0 > Beleid voor processen met hoog risico bij toegang > Mijn standaardwaarde) wordt weergegeven.
73. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
74. Klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
75. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):

- ***Find unknown unwanted programs and trojans (Zoek onbekende ongewenste programma's en trojans).***
- ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***

76. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
77. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.
78. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.
79. Selecteer ***By pattern*** (Op patroon) en voer één voor één de mappen **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:** in en selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten). Klik op ***OK***.
80. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor) en klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
81. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown unwanted programs and trojans (Zoek onbekende ongewenste programma's en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
82. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
83. Klik op het tabblad ***Exclusions*** (Uitsluitingen). Het scherm ***Exclusions*** (Uitsluitingen) wordt weergegeven.
84. Klik op ***Add*** (Toevoegen). Het scherm ***Add/Edit Exclusion Item*** (Uitsluitingsitem toevoegen/bewerken) wordt weergegeven.
85. Selecteer By pattern (Op patroon) en voer één voor één de mappen **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies** in en selecteer ***Also exclude subfolders*** (Submappen ook uitsluiten). Klik op ***OK***.
86. Klik op ***Save*** (Opslaan). Het scherm ***Assigned Policies*** (Toegewezen beleid) wordt geopend.
87. Klik op ***My Default*** (Mijn standaardwaarde) bij ***On Delivery Email Scan Policies*** (Beleid voor direct e-mails scannen). Het scherm ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default*** (VirusScan Enterprise 8.8.0 > Beleid voor direct e-mails scannen > Mijn standaardwaarde) wordt weergegeven.
88. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
89. Klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
90. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken).
    - ***Find unknown program threats and trojans (Zoek onbekende programmabedreigingen en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
    - ***Find attachments with multiple extensions (Zoek bijlagen met meerdere extensies).***

91. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
92. Selecteer ***Disabled*** (Uitgeschakeld) bij ***Artemis (Heuristic network check for suspicious files)*** (Heuristische netwerkcontrole voor verdachte bestanden).
93. Schakel het selectievakje ***Enable on-delivery email scanning*** (Direct e-mails scannen inschakelen) uit onder ***Scanning of email*** (E-mails scannen).
94. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
95. Klik op het tabblad ***Scan Items*** (Scan-items). Het scherm ***Scan Items*** (Scan-items) wordt weergegeven.
96. Schakel de volgende opties uit onder ***Heuristics*** (Heuristieken):
    - ***Find unknown program threats and trojans (Zoek onbekende programmabedreigingen en trojans).***
    - ***Find unknown macro threats (Zoek onbekende macrobedreigingen).***
    - ***Find attachments with multiple extensions (Zoek bijlagen met meerdere extensies).***
97. Schakel het selectievakje ***Detect unwanted programs*** (Ongewenste programma's detecteren) uit onder ***Unwanted programs detection*** (Detectie van ongewenste programma's).
98. Selecteer ***Disabled*** (Uitgeschakeld) bij ***Artemis (Heuristic network check for suspicious files)*** (Heuristische netwerkcontrole voor verdachte bestanden).
99. Schakel het selectievakje ***Enable on-delivery email scanning*** (Direct e-mails scannen inschakelen) uit onder ***Scanning of email*** (E-mails scannen).
100. Klik op ***Save*** (Opslaan). Het scherm ***Assigned Policies*** (Toegewezen beleid) wordt weergegeven.
101. Klik op ***My Default*** (Mijn standaardwaarde) bij ***General Options Policies*** (Beleid voor algemene opties). Het scherm ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** (VirusScan Enterprise 8.8.0 > Beleid voor algemene opties > Mijn standaardwaarde) wordt weergegeven.
102. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
103. Klik op het tabblad ***Display Options*** (Weergaveopties). Het scherm ***Display Options*** (Weergaveopties) wordt weergegeven.
104. Selecteer het volgende onder ***Console options*** (Consoleopties):
    - ***Display managed tasks in the client console (Geef beheerde taken in de clientconsole weer).***
    - ***Disable default AutoUpdate task schedule (Schakel de standaard takenplanning van AutoUpdate uit).***
105. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
106. Klik op het tabblad ***Display Options*** (Weergaveopties). Het scherm ***Display Options*** (Weergaveopties) wordt weergegeven.
107. Selecteer het volgende onder ***Console options*** (Consoleopties).

- ***Display managed tasks in the client console (Geef beheerde taken in de clientconsole weer).***
- ***Disable default AutoUpdate task schedule (Schakel de standaard takenplanning van AutoUpdate uit).***

108. Klik op ***Save*** (Opslaan). Het scherm ***Assigned Policies*** (Toegewezen beleid) wordt weergegeven.
109. Klik op ***My Default*** (Mijn standaardwaarde) bij ***Alert Policies*** (Meldingenbeleid). Het scherm ***VirusScan Enterprise 8.8.0 > Alert Policies > My Default*** (VirusScan Enterprise 8.8.0 > Meldingenbeleid > Mijn standaardwaarde) wordt weergegeven.
110. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).
111. Klik op het tabblad ***Alert Manager Alerts*** (Meldingen meldingsbeheer). Het scherm ***Alert Manager Alerts*** (Meldingen meldingsbeheer) wordt weergegeven.
112. Schakel de selectievakjes ***On-Access Scan*** (Scannen bij toegang), ***On-Demand Scan and scheduled scans*** (Scannen op verzoek en volgens schema), ***Email Scan*** (E-mails scannen) en ***AutoUpdate*** uit onder Components that generate alerts (Onderdelen die meldingen genereren).
113. Selecteer ***Disable alerting*** (Meldingen uitschakelen) onder de opties voor ***Alert Manager*** (Meldingsbeheer).
114. Schakel het selectievakje ***Access Protection*** (Toegangsbeveiliging) uit onder ***Components that generate alerts*** (Onderdelen die meldingen genereren).
115. Klik op ***Additional Alerting Options*** (Aanvullende meldingsopties). Het scherm ***Additional Alerting Options*** (Aanvullende meldingsopties) wordt weergegeven.
116. Selecteer uit het vervolgkeuzemenu ***Severity Filters*** (Filters voor ernst) ***Suppress all alerts (severities 0 to 4)*** (Alle meldingen uitschakelen [ernst 0 t/m 4]).
117. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor) en selecteer het tabblad ***Alert Manager Alerts*** (Meldingen meldingsbeheer). Het scherm ***Alert Manager Alerts*** (Meldingen meldingsbeheer) wordt weergegeven.
118. Schakel de selectievakjes ***On-Access Scan*** (Scannen bij toegang), ***On-Demand Scan and scheduled scans*** (Scannen op verzoek en volgens schema), ***Email Scan*** (E-mails scannen) en ***AutoUpdate*** uit onder Components that generate alerts (Onderdelen die meldingen genereren).
119. Schakel het selectievakje ***Disable alerting*** (Meldingen uitschakelen) in onder de opties voor ***Alert Manager*** (Meldingsbeheer).
120. Schakel het selectievakje ***Access Protection*** (Toegangsbeveiliging) uit onder ***Components that generate alerts*** (Onderdelen die meldingen genereren).
121. Klik op ***Additional Alerting Options*** (Aanvullende meldingsopties). Het scherm Additional Alerting Options (Aanvullende meldingsopties) wordt weergegeven.
122. Selecteer uit het vervolgkeuzemenu ***Severity Filters*** (Filters voor ernst) ***Suppress all alerts (severities 0 to 4)*** (Alle meldingen uitschakelen [ernst 0 t/m 4]).
123. Klik op ***Save*** (Opslaan). Het scherm ***Assigned Policies*** (Toegewezen beleid) wordt weergegeven.

124. Klik op ***My Default*** (Mijn standaardwaarde) bij ***Access Protection Policies*** (Beleid voor toegangsbeveiliging). Het scherm ***VirusScan Enterprise 8.8.0 > Access Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Beleid voor toegangsbeveiliging > Mijn standaardwaarde) wordt weergegeven.

125. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).

126. Klik op het tabblad ***Access Protection*** (Toegangsbeveiliging). Het scherm ***Access Protection*** (Toegangsbeveiliging) wordt weergegeven.

127. Schakel de volgende opties uit onder ***Access protection settings*** (Instellingen voor toegangsbeveiliging):

    - ***Enable access protection (Toegangsbeveiliging inschakelen).***
    - ***Prevent McAfee services from being stopped (Voorkomen dat McAfee-services worden gestopt).***
    - ***Schakel de optie Betere zelfbeveiliging in.***

128. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).

129. Klik op het tabblad ***Access Protection*** (Toegangsbeveiliging). Het scherm ***Access Protection*** (Toegangsbeveiliging) wordt weergegeven.

130. Schakel de volgende opties uit onder ***Access protection settings*** (Instellingen voor toegangsbeveiliging):

    - ***Enable access protection (Toegangsbeveiliging inschakelen).***
    - ***Prevent McAfee services from being stopped (Voorkomen dat McAfee-services worden gestopt).***
    - ***Schakel de optie Betere zelfbeveiliging in.***

131. Klik op ***Save*** (Opslaan). Het scherm ***Assigned Policies*** (Toegewezen beleid) wordt weergegeven.

132. Selecteer ***My Default*** (Mijn standaardwaarde) bij ***Buffer Overflow Protection Policies*** (Beleid voor beveiliging tegen bufferoverloop). Het scherm ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** (VirusScan Enterprise 8.8.0 > Beleid voor beveiliging tegen bufferoverloop > Mijn standaardwaarde) wordt weergegeven.

133. Selecteer ***Workstation*** (Werkstation) uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).

134. Klik op het tabblad ***Buffer Overflow Protection*** (Beveiliging tegen bufferoverloop). Het scherm ***Buffer Overflow Protection*** (Beveiliging tegen bufferoverloop) wordt weergegeven.

135. Schakel het selectievakje ***Show the messages dialog when a buffer overflow is detected*** (Berichtvenster tonen wanneer een bufferoverloop wordt gedetecteerd) uit onder ***Client system warning*** (Clientsysteemwaarschuwing).

136. Schakel het selectievakje ***Enable buffer overflow protection*** (Beveiliging tegen bufferoverloop inschakelen) uit onder ***Buffer overflow settings*** (Instellingen voor bufferoverloop).

137. Selecteer ***Server*** uit de vervolgkeuzelijst ***Settings for*** (Instellingen voor).

138. Klik op het tabblad ***Buffer Overflow Protection*** (Beveiliging tegen bufferoverloop). Het scherm ***Buffer Overflow Protection*** (Beveiliging tegen bufferoverloop) wordt weergegeven.

139. Schakel het selectievakje ***Show the messages dialog when a buffer overflow is detected*** (Berichtvenster tonen wanneer een bufferoverloop wordt gedetecteerd) uit onder ***Client system warning*** (Clientsysteemwaarschuwing).

140. Schakel het selectievakje ***Enable buffer overflow protection*** (Beveiliging tegen bufferoverloop inschakelen) uit onder ***Buffer overflow settings*** (Instellingen voor bufferoverloop).

141. Klik op ***Save*** (Opslaan). Het scherm ***Assigned Policies*** (Toegewezen beleid) wordt weergegeven.

142. Selecteer ***McAfee Agent*** uit het vervolgkeuzemenu ***Product***. Het venster ***Policies*** (Beleid) voor McAfee Agent wordt weergegeven.

143. Klik op ***My Default*** (Mijn standaardwaarde) bij ***Repository*** (Opslagplaats). Het scherm ***McAfee Agent > Repository > My Default*** (McAfee Agent > Opslagplaats > Mijn standaardwaarde) wordt weergegeven.

144. Klik op het tabblad ***Proxy***. Het scherm ***Proxy*** wordt weergegeven.

145. Controleer of ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** (Gebruik Internet Explorer-instellingen [voor Windows]/Instellingen voor systeemvoorkeuren [voor Mac OSX]) is geselecteerd in ***Proxy settings*** (Proxy-instellingen).

146. Klik op ***Save*** (Opslaan). Het scherm ***Assigned Policies*** (Toegewezen beleid) wordt weergegeven.

147. Klik op het tabblad ***Systems*** (Systemen).

148. Selecteer alle clientsystemen (acquisitie, controle en Centricity Cardiology INW-server) waarin u het geconfigureerde beleid wilt implementeren.

149. Selecteer ***Wake Up Agents*** (Agents activeren). Het scherm ***Wake Up Agent*** (Agent activeren) wordt weergegeven.

150. Klik op ***OK***.

151. Meld de ePolicy Orchestrator af.

Richtlijnen voor na de installatie van McAfee ePolicy Orchestrator

Schakel de Loopback-verbinding in. Raadpleeg Schakel de Loopback-verbinding in op pagina 6 voor meer informatie.

Trend Micro OfficeScan Client/Server Edition 10.6 SP2

Overzicht van de installatie

Installeer Trend Micro OfficeScan Client/Server Edition alleen in een Mac-Lab/CardioLab-netwerkomgeving. Trend Micro OfficeScan moet zijn geïnstalleerd op de Anti-virus Management Console Server en vervolgens worden geïmplementeerd op de Centricity Cardiology INW-server en het acquisitie/controlewerkstation als client. Gebruik de volgende instructies om ***Trend Micro OfficeScan Client/Server Edition*** te installeren.

Virusupdates zijn de verantwoordelijkheid van de faciliteit. Zorg dat u de definities regelmatig bijwerkt, zodat de beveiliging van het systeem up-to-date is.

Voorbereiding van de installatie

1. De Trend Micro Anti-Virus Management Console moet worden geïnstalleerd volgens de instructies van Trend Micro en zal naar verwachting goed werken.
2. Doe tijdens het installeren van Trend Micro OfficeScan op de Anti-Virus Management Console-server het volgende:
    a. Schakel ***Enable firewall*** (Firewall activeren) uit in het scherm ***Anti-virus feature*** (Antivirusfunctie).
    b. Kies ***No, Please do not enable assessment mode*** (Nee, schakel de beoordelingsmodus niet in) in het scherm ***Anti-spyware feature*** (Antispywarefunctie).
    c. Schakel de optie ***Enable web reputation policy*** (Activeer webreputatieregels) uit in het scherm ***Web Reputation Feature*** (Webreputatie).
3. Trend Micro OfficeScan wordt niet aanbevolen wanneer de functie ***CO_2*** met PDM in Mac-Lab/CardioLab-systemen wordt gebruikt.
4. Indien Trend Micro OfficeScan vereist is:
    a. Het wordt aanbevolen een aparte Trend Micro Anti-Virus Management Console-server te configureren voor de Mac-Lab/CardioLab-systemen. Een algemene wijziging van de antivirusinstellingen is vereist om de functie ***CO_2*** met PDM in Mac-Lab/CardioLab-systemen te gebruiken.
    b. Als het niet mogelijk is een aparteTrend Micro Anti-Virus Management Console-server te configureren, moet na de installatie de bestaande Trend Micro Anti-Virus Management Console-server worden ingesteld op de algemene instellingen. Deze verandering heeft gevolgen voor alle clientsystemen die zijn verbonden met de bestaande Trend Micro Anti-Virus Management Console-server en moet met ICT-specialisten worden beoordeeld alvorens tot installatie over te gaan.
5. Meld u aan als **Administrator** (Beheerder) of als lid van die groep op alle clientsystemen (acquisitie, controle en INW-server) om de antivirussoftware te installeren.
6. Schakel de Loopback-verbinding uit. Raadpleeg Schakel de Loopback-verbinding uit op pagina 6 voor meer informatie.
7. Configureer de Computerbrowserservice. Raadpleeg Configureer de Computerbrowserservice vóór installatie van de antivirussoftware op pagina 7 voor meer informatie.

Trend Micro OfficeScan - Nieuwe installatieprocedure (de geprefereerde push-installatiemethode)

1. Klik op ***Start > All Programs (Alle programma's) > TrendMicro OfficeScan server - <servernaam> > Office Scan Web Console***.

OPMERKING: Kies vervolgens ***Continue to this website (not recommended)*** (Ga door naar deze website (niet aanbevolen). Selecteer in het scherm Security Alert (Beveiligingsmelding) ***In the future, do not show this warning*** (Laat deze melding in toekomst niet meer zien) en klik op ***OK***.

2. Neem als u een foutmelding krijgt die aangeeft dat deze website niet kan worden vertrouwd, Trend Micro OfficeScan op in uw certificatenoverzicht.
3. Installeer desgevraagd de ***AtxEnc***-invoegtoepassingen. Het scherm Security Warning (Beveiligingswaarschuwing) opent nu.
4. Klik op ***Install*** (Installeren).
5. Voer de gebruikersnaam en het wachtwoord in en klik op ***Log On*** (Aanmelden).
6. Klik desgevraagd op ***Update now*** (Update nu) om de nieuwe widgets te installeren. Wacht totdat de nieuwe widgets zijn bijgewerkt. Het scherm Update gereed zal nu verschijnen.
7. Klik op ***OK***.
8. Klik op de menubalk aan de linkerzijde op ***Networked Computers > Client Installation > Remote*** (Computers in het netwerk > Clientinstallatie > Afstandsbediening).
9. Installeer desgevraagd de ***AtxConsole***-invoegtoepassingen. Het scherm Security Warning (Beveiligingswaarschuwing) opent nu.
10. Klik op ***Install*** (Installeren).
11. Dubbelklik op ***My Company*** (Mijn bedrijf) in het scherm ***Remote Installation*** (Installatie op afstand). Alle domeinen worden weergegeven onder ***My company*** (Mijn bedrijf).
12. Open het domein (bijvoorbeeld: INW) vanuit de lijst. Alle aan dit domein gekoppelde systemen verschijnen.
13. Als de domeinen of systemen niet verschijnen in het scherm ***Domain and Computers*** (Domeinen en computers), doet u per clientsysteem het volgende (Acquisition, Review en INW Server):
    a. Meld u aan als Administrator of als een lid van die groep op alle clientapparaten.
    b. Klik op ***Start > Run*** (Start > Uitvoeren).
    c. Typ ***<Anti-Virus Management Console_server_IP_address>*** en druk op ***Enter***. Desgevraagd voert u gebruikersnaam en wachtwoord in.
    d. Ga naar ***<Anti-Virus Management Console_server_IP _address>\ofsscan*** en dubbelklik op ***AutoPcc.exe***. Desgevraagd voert u gebruikersnaam en wachtwoord in.
    e. Herstart de clientsystemen nadat de installatie is afgerond.

f. Meld u aan als **Administrator** of als een lid van die groep op alle clientapparaten en wacht totdat het Trend Micro OfficeScan-pictogram in het systeemvak blauw is geworden.

g. Sla de resterende stappen van deze procedure over en ga naar de procedure Trend Micro OfficeScan Server Console Configuration.

14. Kies de clientapparaten (Acquisition, Review en INW Server) en klik op ***Add (Toevoegen)***.
15. Typ <domain name>\username en wachtwoord en klik op ***Log on*** (Aanmelden).
16. Kies een voor een de clientapparaten (Acquisition, Review en INW Server) uit het overzicht ***Selected Computers*** (Gekozen computers) en klik op ***Install*** (Installeren).
17. Klik op ***Yes*** (Ja) in het bevestigingsvak.
18. Klik op ***OK*** in het berichtenvak ***Number of clients to which notifications were sent*** (Aantal clients aan wie meldingen zijn gestuurd).
19. Herstart alle clientapparaten (Acquisition, Review en INW Server) en meld u aan als Administrator of als een lid van die groep op alle clientapparaten, en wacht totdat het Trend Micro OfficeScan-pictogramin het systeemvak blauw is en een groen vinkje heeft.
20. Klik op ***Log Off*** (Afmelden) voor het sluiten van de ***OfficeScan Web Console***.

Serverconfiguratie Trend Micro OfficeScan-console

1. Kies ***Start > All Programs > TrendMicro Office Scan server <servernaam> > Office Scan Web Console***. Het scherm ***OfficeScan Login*** (Aanmelden) van Trend Micro verschijnt.
2. Voer de gebruikersnaam en het wachtwoord in en klik op ***Login*** (Aanmelden). Het scherm ***Summary*** (Overzicht) verschijnt.
3. Kies in de balk aan de linkerzijde van het scherm de link ***Networked Computers > Client Management*** (Computers in het netwerk > Clientbeheer).
4. Kies aan de rechterzijde ***OfficeScan Server***.
5. Kies uit de opties in ***Settings*** (Instellingen) voor ***Instellingen*** (Scaninstellingen > Handmatige scaninstellingen). Het scherm ***Manual Scan Settings*** (Handmatige scaninstellingen) verschijnt.
6. Klik op het tab ***Target*** (Doel) en kies alleen de volgende opties, de overige opties schakelt u uit:
   - ***Files to Scan (Te scannen bestanden) > File types scanned by IntelliScan (Bestandstypen gescand door IntelliScan).***
   - ***Scan Settings (Scaninstellingen) > Scan compressed files (Scan de gecomprimeerde bestanden).***
   - ***Scan Settings (Scaninstellingen) > Scan OLE objects (OLE-objecten scannen).***
   - ***Virus/Malware Scan Settings only (Alleen scaninstellingen voor virussen/malware) > Scan boot Area (Opstartgebied scannen).***
   - ***CPU Usage (Processorgebruik) > Low (Laag).***
   - ***Scan Exclusion (Scanuitsluiting) > Enable scan exclusion (Scanuitsluiting inschakelen).***
   - ***Scan Exclusion (Scanuitsluiting) > Apply scan exclusion settings to all scan types (Instellingen voor uitsluitingen toepassen op alle scantypen).***

- ***Scan Exclusion List (Directories) (Scanuitsluitingslijst) > sluit de mappen met geïnstalleerdeTrend Micro producten uit en kies Add path to client Computers Exclusion list (Toevoegen aan de scanuitsluitingslijst).***
- Kies een voor een **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, de mappen **E:** en de **G:** en klik op ***Add*** (Toevoegen).

7. Klik op ***Apply to All Clients*** (Op alle clients toepassen).
8. Klik op ***OK*** op ***De uitsluitingslijst op dit scherm vervangt de uitsluitingslijsten van de clients of domeinen die u eerder hebt gekozen.*** Bericht ***Do you want to proceed?*** (Wilt u doorgaan?).
9. Klik op ***Close*** (Sluiten) ter afsluiting van het scherm ***Manual Scan Settings*** (Handmatige scaninstellingen).
10. Kies in de balk aan de linkerzijde van het scherm de link ***Networked Computers > Client Management*** (Computers in het netwerk > Clientbeheer).
11. Kies aan de rechterzijde ***OfficeScan*** Server.
12. Kies onder ***Settings*** (Instellingen) de opties ***Scan Settings > Real-time Scan Settings*** (Scaninstellingen > Realtimescaninstellingen). Het scherm ***Real-time Scan Settings*** (Realtimescaninstellingen) verschijnt.
13. Klik op het tab ***Target*** (Doel) en kies alleen de volgende opties, de overige opties schakelt u uit:
    - ***Real-Time Scan Settings (Realtimescaninstellingen) > Enable virus/malware scan (Activeer virus/malwarescan).***
    - ***Real-Time Scan Settings (Realtimescaninstellingen)> Enable spyware/grayware scan (Activeer spyware/graywarescan).***
    - ***Files to Scan (Te scannen bestanden) > File types scanned by IntelliScan (Bestandstypen gescand door IntelliScan).***
    - ***Scan Settings (Scaninstellingen) > Scan compressed files (Scan de gecomprimeerde bestanden).***
    - ***Scan Settings (Scaninstellingen) > Scan OLE objects (OLE-objecten scannen).***
    - ***Virus/Malware Scan Settings only (Alleen scaninstellingen voor virussen/malware) > Enable IntelliTrap (IntelliTrap inschakelen).***
    - ***Scan Exclusion (Scanuitsluiting) > Enable scan exclusion (Scanuitsluiting inschakelen).***
    - ***Scan Exclusion (Scanuitsluiting) > Apply scan exclusion settings to all scan types (Instellingen voor uitsluitingen toepassen op alle scantypen).***
    - ***Scan Exclusion List (Directories) (Uitsluitingslijst [mappen]) > Exclude directories where Trend Micro products are installed (Mappen uitsluiten waarin Trend Micro-producten zijn geïnstalleerd).***
    - Zorg ervoor dat ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies*** en de mappen ***E:*** en ***G:*** zijn opgenomen in de ***Exclusion List*** (Uitsluitingslijst).
14. Klik op de tab ***Action*** (Actie).
15. Laat de standaardinstellingen staan en schakel de volgende opties uit:
    - ***Virus/Malware > Display a notification message on the client computer when virus/malware is detected (Laat een melding achter op het clientsysteem indien virus/malware wordt gedetecteerd).***

- ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected (Laat een melding achter op het clientsysteem indien spyware/greyware wordt gedetecteerd).***

16. Klik op ***Apply to All Clients*** (Op alle clients toepassen).
17. Klik op ***Close*** (Sluiten) om het scherm ***Real-time Scan Settings*** (Realtimescaninstellingen) te sluiten.
18. Kies in de balk aan de linkerzijde van het scherm de link ***Networked Computers > Client Management*** (Computers in het netwerk > Clientbeheer).
19. Kies aan de rechterzijde ***OfficeScan Server***.
20. Kies uit de opties in ***Settings*** (Instellingen) ***Scan Settings > Scheduled Scan Settings*** (Scaninstellingen > Instellingen voor ingeplande scans). Het scherm ***Scheduled Scan Settings*** (Instellingen voor ingeplande scans) verschijnt.
21. Klik op het tab ***Target*** (Doel) en kies alleen de volgende opties, de overige opties schakelt u uit:
    - ***Scheduled Scan Settings (Instellingen voor ingeplande scans)> Enable virus/ malware scan (Activeer de virus/malwarescan).***
    - ***Scheduled Scan Settings (Instellingen voor ingeplande scans)> Enable spyware/ grayware scan (Activeer de spyware/graywarescan).***
    - ***Schedule (Planning) > Weekly, every Sunday, Start time (Wekelijks, elke zondag, starttijd): 00:00 uu:mm.***
    - ***Files to Scan (Te scannen bestanden) > File types scanned by IntelliScan (Bestandstypen gescand door IntelliScan).***
    - ***Scan Settings (Scaninstellingen) > Scan compressed files (Scan de gecomprimeerde bestanden).***
    - ***Scan Settings (Scaninstellingen) > Scan OLE objects (OLE-objecten scannen).***
    - ***Virus/Malware Scan Settings only (Alleen scaninstellingen voor virussen/malware) > Scan boot Area (Opstartgebied scannen).***
    - ***CPU Usage (Processorgebruik) > Low (Laag).***
    - ***Scan Exclusion (Scanuitsluiting) > Enable scan exclusion (Scanuitsluiting inschakelen).***
    - ***Scan Exclusion (Scanuitsluiting) > Apply scan exclusion settings to all scan types (Instellingen voor uitsluitingen toepassen op alle scantypen).***
    - ***Scan Exclusion List (Directories) (Uitsluitingslijst [mappen]) > Exclude directories where Trend Micro products are installed (Mappen uitsluiten waarin Trend Micro-producten zijn geïnstalleerd).***
    - Zorg ervoor dat de ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies*** en de mappen ***E:*** en ***G:*** zijn opgenomen in de uitsluitingslijst.
22. Klik op de tab ***Action*** (Actie).
23. Laat de standaardinstellingen staan en schakel de volgende opties uit:
    - ***Virus/Malware > Display a notification message on the client computer when virus/ malware is detected (Laat een melding achter op het clientsysteem indien virus/ malware wordt gedetecteerd).***
    - ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected (Laat een melding achter op het clientsysteem indien spyware/greyware wordt gedetecteerd).***

24. Klik op ***Apply to All Clients*** (Op alle clients toepassen).
25. Klik op ***Close*** (Sluiten) om het scherm ***Scheduled Scan Settings*** (Instellingen voor ingeplande scans) te sluiten.
26. Kies in de balk aan de linkerzijde van het scherm de link ***Networked Computers > Client Management*** (Computers in het netwerk > Clientbeheer).
27. Kies aan de rechterzijde ***OfficeScan Server***.
28. Kies uit de opties in ***Settings*** (Instellingen) ***Scan Settings > Scan Now Settings*** (Scaninstellingen > (Instellingen nu scannen). Het scherm ***Scan Now Settings*** (Instellingen nu scannen) verschijnt.
29. Klik op het tab ***Target*** (Doel) en kies alleen de volgende opties, de overige opties schakelt u uit:
    - ***Scan Now Settings (Instellingen nu scannen) > Enable virus/malware scan (Activeer de virus/malwarescan).***
    - ***Scan Now Settings (Instellingen nu scannen) > Enable spyware/grayware scan (Activeer de spyware/graywarescan).***
    - ***Files to Scan (Te scannen bestanden) > File types scanned by IntelliScan (Bestandstypen gescand door IntelliScan).***
    - ***Scan Settings (Scaninstellingen) > Scan compressed files (Scan de gecomprimeerde bestanden).***
    - ***Scan Settings (Scaninstellingen) > Scan OLE objects (OLE-objecten scannen).***
    - ***Virus/Malware Scan Settings only (Alleen scaninstellingen voor virussen/malware) > Scan boot Area (Opstartgebied scannen).***
    - ***CPU Usage (Processorgebruik) > Low (Laag).***
    - ***Scan Exclusion (Scanuitsluiting) > Enable scan exclusion (Scanuitsluiting inschakelen).***
    - ***Scan Exclusion (Scanuitsluiting) > Apply scan exclusion settings to all scan types (Instellingen voor uitsluitingen toepassen op alle scantypen).***
    - ***Scan Exclusion List (Directories) (Uitsluitingslijst [mappen]) > Exclude directories where Trend Micro products are installed (Mappen uitsluiten waarin Trend Micro-producten zijn geïnstalleerd).***
    - Zorg dat de ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** en ***G:***
30. Klik op ***Apply to All Clients*** (Op alle clients toepassen).
31. Klik op ***Close*** (Sluiten) om het scherm ***Scan Now Settings*** (Instellingen nu scannen) te sluiten.
32. Kies in de balk aan de linkerzijde van het scherm de link ***Networked Computers > Client Management*** (Computers in het netwerk > Clientbeheer).
33. Kies aan de rechterzijde ***OfficeScan Server***.
34. Selecteer uit de opties ***Settings*** (Instellingen) ***Web Reputation Settings*** (Webreputatie-instellingen). Het scherm ***Web Reputation Settings*** (Webreputatie-instellingen) verschijnt.
35. Klik op de tab ***External Clients*** (Externe clients) en schakel ***Enable Web reputation policy on the following operating systems*** (Activeer webreputatieregels op de volgende systemen) uit, indien deze tijdens de installatie is geactiveerd.

36. Klik op de tab ***Internal Clients*** (Interne clients) en deselecteer ***Enable Web reputation policy on the following operating systems*** (Activeer webreputatieregels op de volgende systemen), indien deze tijdens de installatie zijn geselecteerd.
37. Klik op ***Apply to All Clients*** (Op alle clients toepassen).
38. Klik op ***Close*** (Sluiten) om het scherm ***Web Reputation*** (Webreputatie) te sluiten.
39. Kies in de balk aan de linkerzijde van het scherm de link ***Networked Computers > Client Management*** (Computers in het netwerk > Clientbeheer).
40. Kies aan de rechterzijde ***OfficeScan Server***.
41. Kies uit de opties in ***Settings*** (Instellingen) ***Behavior Monitoring Settings*** (Instellingen voor bewaking van gedrag). Het scherm ***Behavior Monitoring Settings*** (Instellingen voor bewaking van gedrag) verschijnt.
42. Schakel de opties ***Enable Malware Behavior Blocking*** (Activeer blokkeren malwaregedrag) en ***Enable Event Monitoring*** (Activeer bewaking van gebeurtenissen) uit.
43. Klik op ***Apply to All Clients*** (Op alle clients toepassen).
44. Klik op ***Close*** (Sluiten) om het scherm ***Behavior Monitoring*** (Bewaking van gedrag) te sluiten.
45. Kies in de balk aan de linkerzijde van het scherm de link ***Networked Computers > Client Management*** (Computers in het netwerk > Clientbeheer).
46. Kies aan de rechterzijde ***OfficeScan Server***.
47. Kies uit de opties in ***Settings*** (Instellingen) ***Device Control Settings*** (Instellingen voor apparaatcontrole). Het scherm ***Device Control Settings*** (Instellingen voor apparaatcontrole) verschijnt.
48. Klik op de tab ***External Clients*** (Externe clients) en schakel de volgende opties uit:
    - ***Notification (Meldingen) > Display a notification message on the client computer when OfficeScan detects unauthorized device access (Laat een melding zien op de clientcomputer wanneer OfficeScan ongeautoriseerde toegang detecteert).***
    - ***Blokkeer de functie AutoRun op USB-opslagapparaten.***
    - ***Activeer Device Control (Apparaatcontrole).***
49. Klik op de tab ***Internal Clients*** (Interne clients) en schakel de volgende opties uit:
    - ***Notification (Meldingen) > Display a notification message on the client computer when OfficeScan detects unauthorized device access (Laat een melding zien op de clientcomputer wanneer OfficeScan ongeautoriseerde toegang detecteert).***
    - ***Blokkeer de functie AutoRun op USB-opslagapparaten.***
    - ***Activeer Device Control (Apparaatcontrole).***
50. Klik op ***Apply to All Clients*** (Op alle clients toepassen).
51. Klik op ***Close*** (Sluiten) om het scherm ***Device Control Settings*** (Instellingen apparaatcontrole) te sluiten.
52. Kies in de balk aan de linkerzijde van het scherm de link ***Networked Computers > Client Management*** (Computers in het netwerk > Clientbeheer).
53. Kies aan de rechterzijde ***OfficeScan Server***.

54. Kies uit de opties in ***Settings*** (Instellingen) ***Privileges and Other Settings*** (Bevoegdheden en andere instellingen).

55. Klik op de tab ***Privileges*** (Bevoegdheden) en kies alleen de volgende opties, schakel de overige opties uit:

    - ***Scan Privileges (Scanbevoegdheden) > Configure Manual Scan Settings (Instellingen voor handmatig scannen configureren).***
    - ***Scan Privileges (Scanbevoegdheden) > Configure Real-time Scan Settings (Instellingen voor realtimescannen configureren).***
    - ***Scan Privileges (Scanbevoegdheden) > Configure Scheduled Scan Settings (Instellingen voor gepland scannen configureren).***
    - ***Proxy Setting Privileges (Bevoegdheden voor proxy-instellingen) > Allow the client user to configure proxy settings (De clientgebruiker kan proxy-instellingen configureren).***
    - ***Uninstallation (Verwijderen) > Require a password for the user to uninstall the OfficeScan Client (Wachtwoord vereist voor het verwijderen van de OfficeScan-clients).*** Voer een bruikbaar wachtwoord in en bevestig dit.
    - ***Unloading (Uitschakelen)> Require a password for the user to unload the OfficeScan client (Wachtwoord vereist voor het uitschakelen van de OfficeScan-client).*** Voer een bruikbaar wachtwoord in en bevestig dit.

56. Klik op de tab ***Other Settings*** (Overige instellingen).

57. Kies ***Client Security Settings > Normal*** (Veiligheidsinstellingen voor client > Normaal) en schakel de overige opties uit.

OPMERKING: Het is belangrijk om de volgende opties uit te schakelen.

- ***Client Self-protection (Beveiliging door de client zelf) > Protect OfficeScan client services (Bescherm OfficeScan-clientservice).***
- ***Client Self-protection (Beveiliging door de client zelf) > Protect files in the OfficeScan client installation folder (Bescherm bestanden in de OfficeScan-installatiemap van de client).***
- ***Client Self-protection (Beveiliging door de client zelf) > Protect OfficeScan client registry keys (Bescherm de OfficeScan-registratienummers van de client).***
- ***Client Self-protection (Beveiliging door de client zelf) > Protect OfficeScan client processes (Bescherm de OfficeScan-processen van de client).***

58. Klik op ***Apply to All Clients*** (Op alle clients toepassen).

59. Klik op ***Close*** (Sluiten) om het scherm ***Privileges and Other Settings*** (Bevoegdheden en andere instellingen) te sluiten.

60. Kies links van het scherm ***Networked Computers > Client Management*** (Computers in het netwerk > Clientbeheer).

61. Kies aan de rechterzijde ***OfficeScan Server***.

62. Kies uit de opties in ***Settings*** (Instellingen) ***Additional Service Settings*** (Aanvullende service-instellingen).

63. Schakel de optie ***Enable service on the following operating systems*** (Activeer service op de volgende systemen) uit.

64. Klik op ***Apply to All Clients*** (Op alle clients toepassen).

65. Klik op ***Close*** (Sluiten) om het scherm ***Additional Service Settings*** (Aanvullende service-instellingen) te sluiten.

66. Kies links van het scherm ***Networked Computers (Computers in het netwerk)> Global Client Settings*** (Algemene clientinstellingen).

67. Kies alleen de volgende opties en schakel de overige opties uit:

    - ***Scan Settings (Scaninstellingen) > Configure Scan settings for large compressed files (Scaninstellingen configureren voor grote gecomprimeerde bestanden).***
    - ***Scan Settings (Scaninstellingen) > Do not scan files in the compressed file if the size exceeds 2 MB (Gecomprimeerde bestanden die groter zijn dan 2 MB niet scannen).***
    - ***Scan Settings (Scaninstellingen) > In a compressed file scan only the first 100 files (In een gecomprimeerd bestand alleen de eerste 100 bestanden scannen).***
    - ***Scan Settings (Scaninstellingen) > Exclude the OfficeScan server database folder from Real-time Scan (Map met OfficeScan-serverdatabase uitsluiten van realtimescan).***
    - ***Scan Settings (Scaninstellingen) > Exclude Microsoft Exchange server folders and files from scans (Mappen van Microsoft Exchange-server uitsluiten van scan).***
    - ***Reserved Disk Space (Gereserveerde schijfruimte) > Reserve 60 MB of disk space for updates (60 MB schijfruimte reserveren voor updates).***
    - ***Proxy Configuration (Proxyconfiguratie > Automatically detect settings (Automatisch instellingen detecteren).***

OPMERKING: Het is belangrijk dat u de optie ***Alert Settings > Display a notification message if the client computer needs to restart to load a kernel driver*** (Meldingsinstellingen > Meldingsbericht weergeven als de clientcomputer opnieuw moet worden gestart om een kernelstuurprogramma te laden) uitschakelt.

68. Klik op ***Save*** (Opslaan).

69. Kies uit het linkervenster ***Updates > Networked Computers > Manual Updates*** (Updates > Computers in het netwerk > Handmatige updates).

70. Kies ***Manually select client*** (Client handmatig selecteren) en klik op ***Select*** (Selecteer).

71. Klik de juiste domeinnaam aan onder ***OfficeScan Server***.

72. Selecteer één clientsysteem per keer en klik op ***Initiate Component Update*** (Start update van onderdeel).

73. Klik ***OK*** in het berichtenvak.

74. Klik op ***Log off*** (Afmelden) en sluit de OfficeScan Web Console.

Installatierichtlijnen voor Trend Micro OfficeScan Post

1. Voer op Acquisition-systemen de volgende stappen uit om Trend Micro te configureren:

    a. Klik op ***Start > Control Panel > Network and Sharing Center*** (Start > Configuratiescherm > Netwerkcentrum).

    b. Klik op ***Change adapter settings*** (Adapterinstellingen wijzigen).

c. Klik met de rechtermuisknop op ***Local Area Connection*** (LAN-verbinding) en kies ***Properties*** (Eigenschappen).

d. Selecteer ***Internet Protocol Version 4 (TCP/IPv4)*** en klik op ***Properties*** (Eigenschappen).

e. Voer het IP-adres _____ in.

f. Sluit alle vensters.

g. Klik op ***Start > Run*** (Start > Uitvoeren) en typ **regedit**.

h. Ga naar ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion***.

i. Klik met de rechtermuisknop op een blanco veld rechts van het scherm en kies ***New > String value*** (Niew > Tekenreekswaarde).

j. Typ **IP Template** voor de naam en klik op **Enter**.

k. Dubbelklik op ***IP Template*** registry (registratie).

l. Voer in het tekstvak ***Value*** (Waarde) het IP-adres van de Local Area Connection (LAN-verbinding) in zoals geregistreerd in stap e.

m. Klik op ***OK***.

n. Sluit de registereditor.

2. Schakel de Loopback-verbinding in. Raadpleeg Schakel de Loopback-verbinding in op pagina 6 voor meer informatie.

3. Configureer de Computerbrowserservice. Raadpleeg Computerbrowserservice configureren na installatie van de antivirussoftware op pagina 7 voor meer informatie.

Algemene instellingen voor Trend Micro-configuraties

OPMERKING: De volgende instructies zijn uitsluitend geschikt voor de functie CO_2 met PDM in Mac-Lab/CardioLab-systemen. Neem de onderstaande stappen eerst met ICT-specialisten door voordat u aan de uitvoering daarvan begint.

1. Ga op de Anti-Virus Management Console-server naar de map ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV***.

2. Open het bestand ***ofcscan.ini*** in een teksteditor.

3. Stel onder ***Global Setting*** (Algemene instellingen) de waarde van de volgende instelling in op **"1"**: [Global Setting] (Algemene instelling)***RmvTmTDI=1***

4. Bewaar en sluit het bestand ofcscan.ini.

5. Klik op ***Start > All Programs (Alle programma's) > TrendMicro OfficeScan server - <servernaam> > Office Scan Web Console***.

6. Voer de gebruikersnaam en het wachtwoord in en klik op ***Log On*** (Aanmelden). Het scherm ***Summary*** (Overzicht) verschijnt.

7. Klik op ***Networked Computers > Global Client Settings*** (Computers in het netwerk > Algemene clientinstellingen).

8. Klik op ***Save*** (Opslaan).
9. Kies links van het scherm ***Updates > Networked Computers > Manual Update*** (Updates > Computers in het netwerk > Handmatige update).
10. Selecteer ***Manually select clients*** (Handmatig selecteren van clients) en klik op ***Select*** (Selecteren).
11. Klik de juiste domeinnaam aan onder ***OfficeScan Server***.
12. Selecteer één clientsysteem per keer en klik op ***Initiate Component Update*** (Start update van onderdeel).
13. Klik ***OK*** in het berichtenvak.
14. Doe het volgende voor elk Acquisition system (Acquisitiesysteem):
    a. Open de registereditor.
    b. Ga naar ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc***.
    c. Zorg ervoor dat de ***RmvTmTDI***-registratie op "**1**" staat.
    d. Ga naar ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.
    e. Verwijder een eventueel aanwezig ***tmtdi***-registratienummer.
    f. Sluit de registereditor.
    g. Herstart de clientsystemen.
    h. Meld u aan op de clientsystemen als administrator of als lid van die groep.
    i. Open op ieder clientsysteem de opdrachtprompt met administrator bevoegdheden en voer "***sc query tmtdi***" in.
    j. Zorg ervoor dat het bericht ***The specified service does not exist as an installed service*** (De opgegeven service komt niet voor als geïnstalleerde service) zichtbaar is.
15. Klik op de Anti-Virus Management Console-server op ***Log off*** (Afmelden) en sluit de OfficeScan Web Console.

Trend Micro OfficeScan Client/Server Edition 11.0 SP1

Installeer Trend Micro OfficeScan Client/Server Edition alleen in een Mac-Lab/CardioLab-netwerkomgeving. Trend Micro OfficeScan moet zijn geïnstalleerd op de Anti-virus Management Console Server en vervolgens worden geïmplementeerd op de Centricity Cardiology INW-server en het acquisitie/controlewerkstation als client. Gebruik de volgende instructies voor het installeren van ***Trend Micro OfficeScan Client/Server Edition 11.0 SP1***.

Virusupdates zijn de verantwoordelijkheid van de faciliteit. Zorg dat u de definities regelmatig bijwerkt, zodat de beveiliging van het systeem up-to-date is.

Voorbereiding van de installatie

1. De Trend Micro Anti-Virus Management Console moet worden geïnstalleerd volgens de instructies van Trend Micro en zal naar verwachting goed werken.

2. Doe tijdens het installeren van Trend Micro OfficeScan op de Anti-Virus Management Console-server het volgende:

   a. Schakel ***Enable firewall*** (Firewall activeren) uit in het scherm ***Anti-virus feature*** (Antivirusfunctie).

   b. Kies ***No, Please do not enable assessment mode*** (Nee, schakel de beoordelingsmodus niet in) in het scherm ***Anti-spyware feature*** (Antispywarefunctie).

   c. Schakel de optie ***Enable web reputation policy*** (Activeer webreputatieregels) uit in het scherm ***Web Reputation Feature*** (Webreputatie).

3. Trend Micro OfficeScan wordt niet aanbevolen indien de functie CO_2 met PDM in Mac-Lab/CardioLab-systemen wordt gebruikt.

4. Indien Trend Micro OfficeScan vereist is:

   a. Het wordt aanbevolen een aparte Trend Micro Anti-Virus Management Console-server te configureren voor de Mac-Lab/CardioLab-systemen. Een algemene verandering van de Anti-Virus-instellingen is vereist voor het gebruik van de functie CO_2 met PDM in Mac-Lab/CardioLab-systemen.

   b. Als het niet mogelijk is een aparteTrend Micro Anti-Virus Management Console-server te configureren, moet na de installatie de bestaande Trend Micro Anti-Virus Management Console-server worden ingesteld op de algemene instellingen. Deze verandering heeft gevolgen voor alle clientsystemen die zijn verbonden met de bestaande Trend Micro Anti-Virus Management Console-server en moet met ICT-specialisten worden beoordeeld alvorens tot installatie over te gaan.

5. Meld u aan als **Administrator** (Beheerder) of als lid van die groep op alle clientsystemen (acquisitie, controle en INW-server) om de antivirussoftware te installeren.

6. Schakel de Loopback-verbinding uit. Raadpleeg Schakel de Loopback-verbinding uit op pagina 6 voor meer informatie.

7. Configureer de Computerbrowserservice. Raadpleeg Configureer de Computerbrowserservice vóór installatie van de antivirussoftware op pagina 7 voor meer informatie.

8. De volgende root en intermediate certificaten zijn vereist voor de installatie van Acquisition-, Review- en INW-clientapparaten:

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

9. Herhaal de volgende tussenstappen om de in stap 8 genoemde vijf root- en intermediaire certificaten te installeren.

   a. Ga naar C***:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***. OPMERKING: Ga op INW naar C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.

   b. Als het hiervoor genoemde pad van de map niet aanwezig is, moet u handmatig de voor de installatie benodigde root en intermediaire certificaten verkrijgen.

c. Dubbelklik op ***AddTrustExternalCARoot.crt*** om dit op de MLCL systemen (Acquisition, Review en INW) te installeren.

d. Open het certificaat en klik op ***Install Certificate*** (Installeer certificaat).

e. Klik op ***Next*** (Volgende) wanneer de ***Certificate Import Wizard*** (Certificaat importeren) verschijnt.

f. Kies in het scherm ***Certificate Store*** (Certificatenwinkel) ***Place all certificates in the following store*** (Zet alle certificaten in de volgende winkel) en klik op ***Browse*** (Bladeren).

g. Bekijk ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** (Overzicht fysieke winkels zien > Betrouwbare rootcertificeringsinstanties > Lokale computer) en klik dan op ***OK***.

h. Klik op ***Next*** (Volgende) op ***Certificate Import Wizard*** (Importeren certificaten).

i. Klik op ***Finish*** (Voltooien). De melding ***The import was successful*** (De import is geslaagd) moet nu zichtbaar zijn.

j. Herhaal stap 9 voor de overige in stap 8 genoemde certificaten.

OPMERKING: Elk certificaat heeft een vervaldatum. De certificaten moeten na het verlopen van de vervaldatum worden vernieuwd en bijgewerkt om ervoor te zorgen dat de OfficeScan-functionaliteiten naar behoren werken.

Trend Micro OfficeScan - Nieuwe installatieprocedure (geprefereerde push-installatiemethode voor 11.0 SP1)

1. Klik op ***Start > All Programs (Alle programma's) > TrendMicro OfficeScan server - <servernaam> > Office Scan Web Console***.

OPMERKING: Kies vervolgens ***Continue to this website (not recommended)*** (Ga door naar deze website (niet aanbevolen). Selecteer in het scherm Security Alert (Beveiligingsmelding) ***In the future, do not show this warning*** (Laat deze melding in toekomst niet meer zien) en klik op ***OK***.

2. Neem als u een foutmelding krijgt die aangeeft dat deze website niet kan worden vertrouwd, Trend Micro OfficeScan op in uw certificatenoverzicht.

3. Installeer desgevraagd de ***AtxEnc***-invoegtoepassingen. Het scherm Security Warning (Beveiligingswaarschuwing) opent nu.

   a. Klik op ***Install*** (Installeren)

4. Voer de gebruikersnaam en het wachtwoord in en klik op ***Log On*** (Aanmelden).

5. Klik desgevraagd op ***Update now*** (Update nu) om de nieuwe widgets te installeren. Wacht totdat de nieuwe widgets zijn bijgewerkt. Het scherm Update gereed zal nu verschijnen.

   a. Klik op ***OK***.

6. Klik in de bovenste menubalk op ***Agents > Agent Installation > Remote*** (Agents > Agents installeren > Op afstand).

7. Installeer desgevraagd de ***AtxConsole***-invoegtoepassingen. Het scherm Security Warning (Beveiligingswaarschuwing) opent nu.

   a. Klik op ***Install*** (Installeren).

8. Dubbelklik op ***OfficeScan Server*** in het scherm ***Remote Installation*** (Installatie op afstand). Alle domeinen worden weergegeven onder de ***OfficeScan Server***.

9. Dubbelklik op het domein (Bijvoorbeeld: INW) vanuit de lijst. Alle aan dit domein gekoppelde systemen verschijnen.

OPMERKING: Indien domeinen of systemen niet worden weergegeven onder het scherm ***Domains and Endpoints*** (Domeinen en eindpunten), ga dan naar Troubleshooting Domains of Systems Not Listed (Probleemoplossingsdomeinen of niet genoemde systemen) in het scherm Domains and Endpoints (Domeinen en eindpunten) op pagina 77 om ze handmatig toe te voegen of voer de installatie direct uit op de clientmachine.

10. Kies de clientapparaten (Acquisition, Review en INW Server) en klik op ***Add (Toevoegen)***.

11. Typ <domain name>\username en wachtwoord en klik op ***Log on*** (Aanmelden).

12. Selecteer de clientapparaten (Acquisition, Review en INW Server) een voor een in het deelvenster ***Selected Computers*** (Gekozen computers) en klik op ***Install*** (Installeren).

13. Klik ***OK*** in het bevestigingsvak.

14. Klik op ***OK*** in het berichtenvak ***Number of clients to which notifications were sent*** (Aantal clients aan wie meldingen zijn gestuurd).

15. Herstart alle clientapparaten (Acquisition, Review en INW Server) en meld u aan als Administrator of als een lid van die groep op alle clientapparaten, en wacht totdat het Trend Micro OfficeScan-pictogramin het systeemvak blauw is en een groen vinkje heeft.

16. Klik op ***Log Off*** (Afmelden) voor het sluiten van de ***OfficeScan Web Console***.

Serverconfiguratie Trend Micro OfficeScan Console voor 11.0 SP1

1. Kies ***Start > All Programs > TrendMicro Office Scan server <servernaam> > Office Scan Web Console***. Het scherm ***OfficeScan Login*** (Aanmelden) van Trend Micro verschijnt.

2. Voer de gebruikersnaam en het wachtwoord in en klik op ***Login*** (Aanmelden). Het scherm ***Summary*** (Overzicht) verschijnt.

3. Kies boven in het scherm ***Agents > Agent Management*** (Agentenbeheer).

4. Kies op de linkerzijde van het scherm ***OfficeScan Server***.

5. Kies uit de opties in ***Settings*** (Instellingen) voor ***Instellingen*** (Scaninstellingen > Handmatige scaninstellingen). Het scherm ***Manual Scan Settings*** (Handmatige scaninstellingen) verschijnt.

6. Klik op het tab ***Target*** (Doel) en kies alleen de volgende opties, de overige opties schakelt u uit:

   - ***Files to Scan (Te scannen bestanden) > File types scanned by IntelliScan (Bestandstypen gescand door IntelliScan).***
   - ***Scan Settings (Scaninstellingen) > Scan compressed files (Scan de gecomprimeerde bestanden).***

- ***Scan Settings (Scaninstellingen) > Scan OLE objects (OLE-objecten scannen).***
- ***Virus/Malware Scan Settings only (Alleen scaninstellingen voor virussen/malware) > Scan boot Area (Opstartgebied scannen).***
- ***CPU Usage (Processorgebruik) > Low (Laag).***

7. Klik op de tab Scan Exclusion (Scanuitsluiting) en kies alleen de volgende opties, schakel de overige opties uit:
   - ***Scan Exclusion (Scanuitsluiting) > Enable scan exclusion (Scanuitsluiting inschakelen).***
   - ***Scan Exclusion (Scanuitsluiting) > Apply scan exclusion settings to all scan types (Instellingen voor uitsluitingen toepassen op alle scantypen).***
   - ***Scan Exclusion List (Directories) (Uitsluitingslijst [mappen]) > Exclude directories where Trend Micro products are installed (Mappen uitsluiten waarin Trend Micro-producten zijn geïnstalleerd).***
   - ***Kies Adds path*** to (Voeg pad toe aan) vanuit het keuzevervolgmenu onder ***Het bewaren van de officescan agent's uitsluitingslijst doet het volgende:***
   - Klik een voor een op **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies** de mappen **E:** en **G:\ +**.
8. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
9. Klik op ***OK*** op ***De uitsluitingslijst op dit scherm vervangt de uitsluitingslijsten van de clients of domeinen die u eerder hebt gekozen.*** Bericht ***Do you want to proceed?*** (Wilt u doorgaan?).
10. Klik op ***Close*** (Sluiten) ter afsluiting van het scherm ***Manual Scan Settings*** (Handmatige scaninstellingen).
11. Kies boven in het scherm de koppeling ***Agent > Agent Management*** (Agentenbeheer).
12. Kies op de linkerzijde van het scherm ***OfficeScan*** Server.
13. Kies onder ***Settings*** (Instellingen) de opties ***Scan Settings > Real-time Scan Settings*** (Scaninstellingen > Realtimescaninstellingen). Het scherm ***Real-time Scan Settings*** (Realtimescaninstellingen) verschijnt.
14. Klik op het tab ***Target*** (Doel) en kies alleen de volgende opties, de overige opties schakelt u uit:
    - ***Real-Time Scan Settings (Realtimescaninstellingen) > Enable virus/malware scan (Activeer virus/malwarescan).***
    - ***Real-Time Scan Settings (Realtimescaninstellingen)> Enable spyware/grayware scan (Activeer spyware/graywarescan).***
    - ***Files to Scan (Te scannen bestanden) > File types scanned by IntelliScan (Bestandstypen gescand door IntelliScan).***
    - ***Scan Settings (Scaninstellingen) > Scan compressed files (Scan de gecomprimeerde bestanden).***
    - ***Scan Settings (Scaninstellingen) > Scan OLE objects (OLE-objecten scannen).***
    - ***Virus/Malware Scan Settings only (Alleen scaninstellingen voor virussen/malware) > Enable IntelliTrap (IntelliTrap inschakelen).***

15. Klik op de tab Scan Exclusion (Scanuitsluiting) en kies alleen de volgende opties, schakel de overige opties uit:
    - ***Scan Exclusion (Scanuitsluiting) > Enable scan exclusion (Scanuitsluiting inschakelen).***
    - ***Scan Exclusion (Scanuitsluiting) > Apply scan exclusion settings to all scan types (Instellingen voor uitsluitingen toepassen op alle scantypen).***
    - ***Scan Exclusion List (Directories) (Uitsluitingslijst [mappen]) > Exclude directories where Trend Micro products are installed (Mappen uitsluiten waarin Trend Micro-producten zijn geïnstalleerd).***
    - Zorg ervoor dat ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies*** en de mappen ***E:*** en ***G:*** zijn opgenomen in de ***Exclusion List*** (Uitsluitingslijst).
16. Klik op de tab ***Action*** (Actie).
17. Laat de standaardinstellingen staan en schakel de volgende opties uit:
    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected (Plaats op eindpunten een melding wanneer virus/malware is gedetecteerd).***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected (Plaats op eindpunten een melding wanneer spyware/grayware is gedetecteerd).***
18. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
19. Klik op ***Close*** (Sluiten) om het scherm ***Real-time Scan Settings*** (Realtimescaninstellingen) te sluiten.
20. Kies boven in het scherm ***Agents > Agent Management*** (Agentenbeheer).
21. Kies op de linkerzijde van het scherm ***OfficeScan Server***.
22. Kies uit de opties in ***Settings*** (Instellingen) ***Scan Settings > Scheduled Scan Settings*** (Scaninstellingen > Instellingen voor ingeplande scans). Het scherm ***Scheduled Scan Settings*** (Instellingen voor ingeplande scans) verschijnt.
23. Klik op het tab ***Target*** (Doel) en kies alleen de volgende opties, de overige opties schakelt u uit:
    - ***Scheduled Scan Settings (Instellingen voor ingeplande scans)> Enable virus/malware scan (Activeer de virus/malwarescan).***
    - ***Scheduled Scan Settings (Instellingen voor ingeplande scans)> Enable spyware/grayware scan (Activeer de spyware/graywarescan).***
    - ***Schedule (Planning) > Weekly, every Sunday, Start time (Wekelijks, elke zondag, starttijd): 00:00 uu:mm.***
    - ***Files to Scan (Te scannen bestanden) > File types scanned by IntelliScan (Bestandstypen gescand door IntelliScan).***
    - ***Scan Settings (Scaninstellingen) > Scan compressed files (Scan de gecomprimeerde bestanden).***
    - ***Scan Settings (Scaninstellingen) > Scan OLE objects (OLE-objecten scannen).***
    - ***Virus/Malware Scan Settings only (Alleen scaninstellingen voor virussen/malware) > Scan boot Area (Opstartgebied scannen).***
    - ***CPU Usage (Processorgebruik) > Low (Laag).***

24. Klik op de tab ***Scan Exclusion*** (Scanuitsluiting) en kies alleen de volgende opties en schakel de overige opties uit:
    - ***Scan Exclusion (Scanuitsluiting) > Enable scan exclusion (Scanuitsluiting inschakelen).***
    - ***Scan Exclusion (Scanuitsluiting) > Apply scan exclusion settings to all scan types (Instellingen voor uitsluitingen toepassen op alle scantypen).***
    - ***Scan Exclusion List (Directories) (Uitsluitingslijst [mappen]) > Exclude directories where Trend Micro products are installed (Mappen uitsluiten waarin Trend Micro-producten zijn geïnstalleerd).***
    - Zorg ervoor dat de ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies*** en de mappen ***E:*** en ***G:*** zijn opgenomen in de uitsluitingslijst.
25. Klik op de tab ***Action*** (Actie).
26. Laat de standaardinstellingen staan en schakel de volgende opties uit:
    - ***Virus/Malware > Display a notification message on the endpoints when virus/malware is detected (Plaats op eindpunten een melding wanneer virus/malware is gedetecteerd).***
    - ***Spyware/Grayware > Display a notification message on the endpoints when spyware/grayware is detected (Plaats op eindpunten een melding wanneer spyware/grayware is gedetecteerd).***
27. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
28. Klik op ***Close*** (Sluiten) om het scherm ***Scheduled Scan Settings*** (Instellingen voor ingeplande scans) te sluiten.
29. Kies boven in het scherm ***Agents > Agent Management*** (Agentenbeheer).
30. Kies op de linkerzijde van het scherm ***OfficeScan Server***.
31. Kies uit de opties in ***Settings*** (Instellingen) ***Scan Settings > Scan Now Settings*** (Scaninstellingen > (Instellingen nu scannen). Het scherm ***Scan Now Settings*** (Instellingen nu scannen) verschijnt.
32. Klik op het tab ***Target*** (Doel) en kies alleen de volgende opties, de overige opties schakelt u uit:
    - ***Scan Now Settings (Instellingen nu scannen) > Enable virus/malware scan (Activeer de virus/malwarescan).***
    - ***Scan Now Settings (Instellingen nu scannen) > Enable spyware/grayware scan (Activeer de spyware/graywarescan).***
    - ***Files to Scan (Te scannen bestanden) > File types scanned by IntelliScan (Bestandstypen gescand door IntelliScan).***
    - ***Scan Settings (Scaninstellingen) > Scan compressed files (Scan de gecomprimeerde bestanden).***
    - ***Scan Settings (Scaninstellingen) > Scan OLE objects (OLE-objecten scannen).***
    - ***Virus/Malware Scan Settings only (Alleen scaninstellingen voor virussen/malware) > Scan boot Area (Opstartgebied scannen).***
    - ***CPU Usage (Processorgebruik) > Low (Laag).***

33. Klik op de tab ***Scan Exclusion*** (Scanuitsluiting) en kies alleen de volgende opties en schakel de overige opties uit:
    - ***Scan Exclusion (Scanuitsluiting) > Enable scan exclusion (Scanuitsluiting inschakelen).***
    - ***Scan Exclusion (Scanuitsluiting) > Apply scan exclusion settings to all scan types (Instellingen voor uitsluitingen toepassen op alle scantypen).***
    - ***Scan Exclusion List (Directories) (Uitsluitingslijst [mappen]) > Exclude directories where Trend Micro products are installed (Mappen uitsluiten waarin Trend Micro-producten zijn geïnstalleerd).***
    - Zorg ervoor dat ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies*** en de mappen ***E:*** en ***G:*** zijn opgenomen in de Exclusion List (Uitsluitingslijst).
34. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
35. Klik op ***Close*** (Sluiten) om het scherm ***Scan Now Settings*** (Instellingen nu scannen) te sluiten.
36. Kies boven in het scherm ***Agents > Agent Management*** (Agentenbeheer).
37. Kies op de linkerzijde van het scherm ***OfficeScan Server***.
38. Selecteer uit de opties ***Settings*** (Instellingen) ***Web Reputation Settings*** (Webreputatie-instellingen). Het scherm ***Web Reputation Settings*** (Webreputatie-instellingen) verschijnt.
39. Klik op het tabblad ***External Agents*** (Externe agenten) en deselecteer ***Enable Web reputation policy on the following operating systems*** (Activeer webreputatieregels op de volgende besturingssystemen), als deze optie tijdens de installatie is geselecteerd.
40. Klik op de tab ***Internal Agents*** (Interne agenten) en deselecteer ***Enable Web reputation policy on the following operating systems*** (Activeer webreputatieregels op de volgende besturingssystemen), indien deze tijdens de installatie is geselecteerd.
41. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
42. Klik op ***Close*** (Sluiten) om het scherm ***Web Reputation*** (Webreputatie) te sluiten.
43. Kies boven in het scherm ***Agents > Agent Management*** (Agentenbeheer).
44. Kies op de linkerzijde van het scherm ***OfficeScan Server***.
45. Kies uit de opties in ***Settings*** (Instellingen) ***Behavior Monitoring Settings*** (Instellingen voor bewaking van gedrag). Het scherm ***Behavior Monitoring Settings*** (Instellingen voor bewaking van gedrag) verschijnt.
46. Deselecteer de opties ***Enable Malware Behavior Blocking for known and potential threats*** (Activeer blokkeren malware gedrag voor bekende en potentiële bedreigingen) en ***Enable Event Monitoring*** (Activeer bewaking van gebeurtenissen).
47. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
48. Klik op ***Close*** (Sluiten) om het scherm ***Behavior Monitoring*** (Bewaking van gedrag) te sluiten.
49. Kies boven in het scherm ***Agents > Agent Management*** (Agentenbeheer).
50. Kies op de linkerzijde van het scherm ***OfficeScan Server***.
51. Kies uit de opties in ***Settings*** (Instellingen) ***Device Control Settings*** (Instellingen voor apparaatcontrole). Het scherm ***Device Control Settings*** (Instellingen voor apparaatcontrole) verschijnt.

52. Klik op de tab ***External Agents*** (Externe agenten) en deselecteer de volgende opties:
    - ***Notification (Melding) > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Laat een melding op eindpunten zien wanneer OfficeScan ongeautoriseerde toegang detecteert).***
    - ***Blokkeer de functie AutoRun op USB-opslagapparaten.***
53. Klik op de tab ***Internal Agents*** (Interne agenten) en deselecteer de volgende opties:
    - ***Notification (Melding) > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Laat een melding op eindpunten zien wanneer OfficeScan ongeautoriseerde toegang detecteert).***
    - ***Blokkeer de functie AutoRun op USB-opslagapparaten.***
54. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
55. Klik op ***Close*** (Sluiten) om het scherm ***Device Control Settings*** (Instellingen apparaatcontrole) te sluiten.
56. Kies opnieuw uit de ***Settings*** (Instellingen) opties ***Device Control Settings*** (Instellingen apparaatcontrole). Het scherm ***Device Control Settings*** (Instellingen voor apparaatcontrole) verschijnt.
57. Klik op de tab ***External Agents*** (Externe agenten) en deselecteer ***Enable Device Control*** (Activeer apparaatcontrole).
58. Klik op de tab ***Internal Agents*** (Interne agenten) en deselecteer ***Enable Device Control*** (Activeer apparaatcontrole).
59. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
60. Klik op ***Close*** (Sluiten) om het scherm ***Device Control Settings*** (Instellingen apparaatcontrole) te sluiten.
61. Kies boven in het scherm ***Agents > Agent Management*** (Agentenbeheer).
62. Kies op de linkerzijde van het scherm ***OfficeScan Server***.
63. Kies uit de opties in ***Settings*** (Instellingen) ***Privileges and Other Settings*** (Bevoegdheden en andere instellingen).
64. Klik op de tab ***Privileges*** (Bevoegdheden) en kies alleen de volgende opties, schakel de overige opties uit:
    - ***Scans > Configure Manual Scan Settings (Instellingen voor handmatig scannen configureren).***
    - ***Scans > Configure Real-time Scan Settings (Instellingen voor realtimescannen configureren).***
    - ***Scans > Configure Scheduled Scan Settings (Instellingen voor gepland scannen configureren).***
    - ***Proxy Settings > Sta gebruikers toe proxy settings te configureren.***
    - ***Uninstallation (deïnstallatie) > wachtwoord vereist.*** Voer een bruikbaar wachtwoord in en bevestig dit.
    - ***Unload and Unlock (Uitschakelen en ontgrendelen) > Wachtwoord vereist.*** Voer een bruikbaar wachtwoord in en bevestig dit.
65. Klik op de tab ***Other Settings*** (Overige instellingen).

66. Selecteer ***OfficeScan Agent Security Settings > Normal*** (OfficeScan-agentbeveiligingsinstellingen > Normaal): ***Allow users to access OfficeScan agent files and registries*** (Geef gebruikers toegang tot OfficeScan-agentbestanden en -registraties) en schakel de overige opties uit.

OPMERKING: Het is belangrijk om de volgende opties uit te schakelen.

- ***OfficeScan Agent Self-protection (Zelfbecherming agent OfficeScan) > Protect OfficeScan agent services (Bescherm OfficeScan-agentservices).***
- ***OfficeScan Agent Self-protection (Zelfbecherming agent OfficeScan)> Protect files in the OfficeScan agent installation folder (Bescherm bestanden in de OfficeScan-agentinstallatiemap).***
- ***OfficeScan Agent Self-protection (Zelfbecherming agent OfficeScan)> Protect OfficeScan agent registry keys (Bescherm de OfficeScan-agentregistratienummers).***
- ***OfficeScan Agent Self-protection (Zelfbeveiliging OfficeScan-agent)> Protect OfficeScan agent processes (Bescherm de OfficeScan-agentprocessen).***

67. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
68. Klik op ***Close*** (Sluiten) om het scherm ***Privileges and Other Settings*** (Bevoegdheden en andere instellingen) te sluiten.
69. Kies boven in het scherm ***Agents > Agent Management*** (Agentbeheer).
70. Kies op de linkerzijde van het scherm ***OfficeScan Server***.
71. Kies uit de opties in ***Settings*** (Instellingen) ***Additional Service Settings*** (Aanvullende service-instellingen).
72. Schakel de optie ***Enable service on the following operating systems*** (Activeer service op de volgende systemen) uit.
73. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
74. Klik op ***Close*** (Sluiten) om het scherm ***Additional Service Settings*** (Aanvullende service-instellingen) te sluiten.
75. Kies boven in het scherm ***Agents > Global Agent Settings*** (Algemene agentinstellingen).
76. Kies alleen de volgende opties en schakel de overige opties uit:
    - ***Scan Settings for Large Compressed Files (Scaninstellingen voor grote gecomprimeerde bestanden) > Configure Scan settings for large compressed files (Configureer scaninstellingen voor grote gecomprimeerde bestanden).***
    - ***Scan Settings for Large Compressed Files > Do not scan files in the compressed file if the size exceeds 2 MB*** (Scaninstellingen voor grote gecomprimeerde bestanden > Gecomprimeerde bestanden die groter zijn dan 2 MB, niet scannen). ***Real-Time Scan*** en ***Manual Scan/Schedule Scan/Scan Now*** (Handmatige scan/Geplande scan en Nu scannen).
    - ***Scan Settings for Large Compressed Files (Scaninstellingen voor grote gecomprimeerde bestanden) > In a compressed file scan only the first 100 files (In een gecomprimeerd bestand alleen de eerste 100 bestanden scannen). Real-Time Scan*** en ***Manual Scan/Schedule Scan/Scan Now*** (Handmatige scan/Geplande scan en Nu scannen).

- ***Scan Settings (Scaninstellingen) > Exclude the OfficeScan server database folder from Real-time Scan (Map met OfficeScan-serverdatabase uitsluiten van realtimescan).***
- ***Scan Settings (Scaninstellingen) > Exclude Microsoft Exchange server folders and files from scans (Mappen van Microsoft Exchange-server uitsluiten van scan).***
- ***Reserved Disk Space (Gereserveerde schijfruimte) > Reserve 60 MB of disk space for updates (60 MB schijfruimte reserveren voor updates).***
- ***Proxy Configuration (Proxyconfiguratie > Automatically detect settings (Automatisch instellingen detecteren).***

OPMERKING: Het is belangrijk dat u de optie ***Alert Settings > Display a notification message*** (Meldingsinstellingen > Meldingsbericht weergeven) uitschakelt als het eindpunt opnieuw moet worden gestart om een kernelstuurprogramma te laden.

77. Klik op ***Save*** (Opslaan).
78. Kies boven in het scherm ***Updates > Agents > Manual Updates*** (Handmatige updates).
79. Selecteer ***Manually select agents*** (Agenten handmatig selecteren) en klik op ***Select*** (Selecteer).
80. Dubbelklik op de gewenste domeinnaam onder ***OfficeScan Server***.
81. Selecteer een voor een de clientsystemen en klik op ***Initiate Update*** (Start update).
82. Klik ***OK*** in het berichtenvak.
83. Klik op ***Log off*** (Afmelden) en sluit de OfficeScan Web Console.

Algemene instellingen voor Trend Micro-configuraties

OPMERKING: De volgende instructies zijn uitsluitend geschikt voor de functie CO_2 met PDM in Mac-Lab/CardioLab-systemen. Neem de onderstaande stappen eerst met ICT-specialisten door voordat u aan de uitvoering daarvan begint.

1. Ga op de Anti-Virus Management Console-server naar de map C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV.
2. Open het bestand ***ofcscan.ini*** in een teksteditor.
3. Zet bij Global Setting (Algemene instelling) de volgende waarde op "**1**": [Global Setting] (Algemene instelling) ***RmvTmTDI=1***
4. Bewaar en sluit het bestand ofcscan.ini.
5. Klik op ***Start > All Programs > TrendMicro OfficeScan server - <server name> > OfficeScan Web Console***.
6. Voer de juiste gebruikersnaam en het wachtwoord in en klik op ***Log On*** (Aanmelden). Het scherm ***Dashboard*** verschijnt.
7. Klik op ***Agents > Global Agent Settings*** (Algemene agentinstellingen).
8. Klik op ***Save*** (Opslaan).
9. Selecteer links van het scherm ***Updates > Agents > Manual Update*** (Handmatige update).

10. Selecteer ***Manually select clients*** (Clients handmatig selecteren) en klik op ***Select*** (Selecteer).
11. Klik de gewenste domeinnaam onder ***OfficeScan Server***.
12. Kies een voor een de clientsystemen en klik op ***Initiate Update*** (Start update).
13. Klik op ***OK*** in het berichtenvak.
14. Doe het volgende voor elk Acquisition system (Acquisitiesysteem):
    a. Open de registereditor.
    b. Ga naar ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc.***
    c. Zorg ervoor dat het ***RmvTmTDI***-registratienummer op "***1***" staat.
    d. Ga naar ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.
    e. Verwijder het eventuele ***tmtdi***-registratienummer.
    f. Sluit de registereditor.
    g. Herstart de clientsystemen.
    h. Meld u aan op de clientsystemen als administrator of als lid van die groep.
    i. Open op elk clientsysteem de opdrachtprompt met administratorbevoegdheden en voer "***sc query tmtdi***" in.
    j. Zorg ervoor dat de melding ***The specified service does not exist as an installed service*** (De opgegeven service is niet als geïnstalleerde service aanwezig) zichtbaar is.
15. Klik op de Anti-Virus Management Console-server op ***Log off*** (Afmelden) en sluit de OfficeScan Web Console.

Installatierichtlijnen voor Trend Micro OfficeScan Post

1. Schakel de Loopback-verbinding in. Raadpleeg Schakel de Loopback-verbinding in op pagina 6 voor meer informatie.
2. Configureer de Computerbrowserservice. Raadpleeg Computerbrowserservice configureren na installatie van de antivirussoftware op pagina 7 voor meer informatie.

Trend Micro OfficeScan Client/Server Edition XG 12.0

Overzicht van de installatie

Installeer Trend Micro OfficeScan Client/Server Edition alleen in een Mac-Lab/CardioLab-netwerkomgeving. Trend Micro OfficeScan moet zijn geïnstalleerd op de Anti-virus Management Console Server en vervolgens worden geïmplementeerd op de Centricity Cardiology INW-server en het acquisitie/controlewerkstation als client. Gebruik de volgende instructies voor het installeren van ***Trend Micro OfficeScan Client/Server Edition XG 12.0***.

Virusupdates zijn de verantwoordelijkheid van de faciliteit. Zorg dat u de definities regelmatig bijwerkt, zodat de beveiliging van het systeem up-to-date is.

Voorbereiding van de installatie

OPMERKING: Internet Explorer 10 is minimaal benodigd als IE browser om de OfficeScan manager uit te voeren.

1. De Trend Micro Anti-Virus Management Console moet worden geïnstalleerd volgens de instructies van Trend Micro en zal naar verwachting goed werken.
2. Doe tijdens het installeren van Trend Micro OfficeScan op de Anti-Virus Management Console-server het volgende:
   a. Schakel ***Enable firewall*** (Firewall activeren) uit in het scherm ***Anti-virus feature*** (Antivirusfunctie).
   b. Kies ***No, Please do not enable assessment mode*** (Nee, schakel de beoordelingsmodus niet in) in het scherm ***Anti-spyware feature*** (Antispywarefunctie).
   c. Schakel de optie ***Enable web reputation policy*** (Activeer webreputatieregels) uit in het scherm ***Web Reputation Feature*** (Webreputatie).
3. Meld u aan als **Administrator** (Beheerder) of als lid van die groep op alle clientsystemen (acquisitie, controle en INW-server) om de antivirussoftware te installeren.
4. Schakel de Loopback-verbinding uit. Raadpleeg Schakel de Loopback-verbinding uit op pagina 6 voor meer informatie.
5. Configureer de Computerbrowserservice. Raadpleeg Configureer de Computerbrowserservice vóór installatie van de antivirussoftware op pagina 7 voor meer informatie.
6. De volgende root en intermediate certificaten zijn vereist voor de installatie van Acquisition-, Review- en INW-clientapparaten:
   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt

7. Herhaal de volgende tussenstappen om de vereiste vijf basis- en intermediaire certificaten te installeren zoals genoemd in stap 6.

    a. Ga naar C***:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***.
    OPMERKING: Ga op INW naar
    C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.

    b. Als het hiervoor genoemde pad van de map niet aanwezig is, moet u handmatig de voor de installatie benodigde root en intermediaire certificaten verkrijgen.

    c. Dubbelklik op ***AddTrustExternalCARoot.crt*** om dit op de MLCL systemen (Acquisition, Review en INW) te installeren.

    d. Open het certificaat en klik op ***Install Certificate*** (Installeer certificaat).

    e. Klik op ***Next*** (Volgende) wanneer de ***Certificate Import Wizard*** (Certificaat importeren) verschijnt.

    f. Kies in het scherm ***Certificate Store*** (Certificatenwinkel) ***Place all certificates in the following store*** (Zet alle certificaten in de volgende winkel) en klik op ***Browse*** (Bladeren).

    g. Bekijk ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** (Overzicht fysieke winkels zien > Betrouwbare rootcertificeringsinstanties > Lokale computer) en klik dan op ***OK***.

    h. Klik op ***Next*** (Volgende) op ***Certificate Import Wizard*** (Importeren certificaten).

    i. Klik op ***Finish*** (Voltooien). De melding ***The import was successful*** (De import is geslaagd) moet nu zichtbaar zijn.

    j. Herhaal stap 7 voor de andere in stap 6 genoemde certificaten.

OPMERKING: Elk certificaat heeft een vervaldatum. De certificaten moeten na het verlopen van de vervaldatum worden vernieuwd en bijgewerkt om ervoor te zorgen dat de OfficeScan-functionaliteiten naar behoren werken.

Trend Micro OfficeScan - Nieuwe installatieprocedure (geprefereerde push-installatiemethode voor 12.0)

1. Klik op ***Start > All Programs (Alle programma's) > TrendMicro OfficeScan server - <servernaam> > Office Scan Web Console***.

OPMERKING: Kies vervolgens ***Continue to this website (not recommended)*** (Ga door naar deze website (niet aanbevolen). Selecteer in het scherm Security Alert (Beveiligingsmelding) ***In the future, do not show this warning*** (Laat deze melding in toekomst niet meer zien) en klik op ***OK***.

2. Neem als u een foutmelding krijgt die aangeeft dat deze website niet kan worden vertrouwd, Trend Micro OfficeScan op in uw certificatenoverzicht.

3. Installeer desgevraagd de ***AtxEnc***-invoegtoepassingen. Het scherm Security Warning (Beveiligingswaarschuwing) opent nu.

    a. Klik op ***Install*** (Installeren)

4. Voer de gebruikersnaam en het wachtwoord in en klik op ***Log On*** (Aanmelden).

5. Klik desgevraagd op ***Update now*** (Update nu) om de nieuwe widgets te installeren. Wacht totdat de nieuwe widgets zijn bijgewerkt. Het scherm Update gereed zal nu verschijnen.

   a. Klik op ***OK***.

6. Klik in de bovenste menubalk op ***Agents > Agent Installation > Remote*** (Agents > Agents installeren > Op afstand).

7. Installeer desgevraagd de ***AtxConsole***-invoegtoepassingen. Het scherm Security Warning (Beveiligingswaarschuwing) opent nu.

   a. Klik op ***Install*** (Installeren).

8. Dubbelklik op ***My Company*** (Mijn bedrijf) in het scherm ***Remote Installation*** (Installatie op afstand). Alle domeinen worden weergegeven onder de ***OfficeScan Server***.

9. Dubbelklik op het domein (Bijvoorbeeld: INW) vanuit de lijst. Alle aan dit domein gekoppelde systemen verschijnen.

OPMERKING: Indien domeinen of systemen niet worden weergegeven onder het scherm ***Domains and Endpoints*** (Domeinen en eindpunten), ga dan naar Troubleshooting Domains of Systems Not Listed (Probleemoplossingsdomeinen of niet genoemde systemen) in het scherm Domains and Endpoints (Domeinen en eindpunten) op pagina 77 om ze handmatig toe te voegen of voer de installatie direct uit op de clientmachine.

10. Kies de clientapparaten (Acquisition, Review en INW Server) en klik op ***Add (Toevoegen)***.

11. Typ <domain name>\username en wachtwoord en klik op ***Log on*** (Aanmelden).

12. Selecteer de clientapparaten (Acquisition, Review en INW Server) een voor een in het deelvenster ***Selected Computers*** (Gekozen computers) en klik op ***Install*** (Installeren).

13. Klik op ***Yes*** (Ja) in het bevestigingsvak.

14. Klik op ***OK*** in het berichtenvak ***Number of agents to which notifications were sent*** (Aantal agenten aan wie een melding is gestuurd).

15. Herstart alle clientapparaten (Acquisition, Review en INW Server) en meld u aan als Administrator of als een lid van die groep op alle clientapparaten, en wacht totdat het Trend Micro OfficeScan-pictogramin het systeemvak blauw is en een groen vinkje heeft.

16. Klik op ***Log Off*** (Afmelden) voor het sluiten van de ***OfficeScan Web Console***.

Serverconfiguratie Trend Micro OfficeScan Console voor 12.0

1. Kies ***Start > All Programs > TrendMicro Office Scan server <servernaam> > Office Scan Web Console***. Het scherm ***OfficeScan Login*** (Aanmelden) van Trend Micro verschijnt.

2. Voer de gebruikersnaam en het wachtwoord in en klik op ***Login*** (Aanmelden). Het scherm ***Summary*** (Overzicht) verschijnt.

3. Kies boven in het scherm ***Agents > Agent Management*** (Agentenbeheer).

4. Kies op de linkerzijde van het scherm ***OfficeScan Server***.

5. Kies uit de opties in ***Settings*** (Instellingen) voor ***Instellingen*** (Scaninstellingen > Handmatige scaninstellingen). Het scherm ***Manual Scan Settings*** (Handmatige scaninstellingen) verschijnt.

6. Klik op het tab ***Target*** (Doel) en kies alleen de volgende opties, de overige opties schakelt u uit:

   - ***Files to Scan (Te scannen bestanden) > File types scanned by IntelliScan (Bestandstypen gescand door IntelliScan).***
   - ***Scan Settings (Scaninstellingen) > Scan compressed files (Scan de gecomprimeerde bestanden).***
   - ***Scan Settings (Scaninstellingen) > Scan OLE objects (OLE-objecten scannen).***
   - ***Virus/Malware Scan Settings only (Alleen scaninstellingen voor virussen/malware) > Scan boot Area (Opstartgebied scannen).***
   - ***CPU Usage (Processorgebruik) > Low (Laag).***

7. Klik op de tab Scan Exclusion (Scanuitsluiting) en kies alleen de volgende opties, schakel de overige opties uit:

   - ***Scan Exclusion (Scanuitsluiting) > Enable scan exclusion (Scanuitsluiting inschakelen).***
   - ***Scan Exclusion (Scanuitsluiting) > Apply scan exclusion settings to all scan types (Instellingen voor uitsluitingen toepassen op alle scantypen).***
   - ***Scan Exclusion List (Directories) (Uitsluitingslijst (mappen)) > Exclude directories where Trend Micro products are installed (Mappen uitsluiten waarin Trend Micro-producten zijn geïnstalleerd) en selecteer Add path to agent Computers Exclusion list (Voeg pad toe aan de uitsluitingslijst voor computers van agenten).***
   - ***Kies Adds path*** to (Voeg pad toe aan) vanuit het keuzevervolgmenu onder ***Het bewaren van de officescan agent's uitsluitingslijst doet het volgende:***
   - Kies een voor een **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, de mappen **E:** en de **G:** en klik op ***Add*** (Toevoegen).

8. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).

9. Klik op ***OK*** bij ***The exclusion list on this screen will replace the exclusion list on the agents or domains you selected in the client tree earlier*** (De uitsluitingslijst op dit scherm vervangt de uitsluitingslijsten van de agenten of domeinen die u eerder hebt gekozen). Bericht ***Do you want to proceed?*** (Wilt u doorgaan?).

10. Klik op ***Close*** (Sluiten) ter afsluiting van het scherm ***Manual Scan Settings*** (Handmatige scaninstellingen).

11. Kies boven in het scherm de koppeling ***Agent > Agent Management*** (Agentenbeheer).

12. Kies op de linkerzijde van het scherm ***OfficeScan*** Server.

13. Kies onder ***Settings*** (Instellingen) de opties ***Scan Settings > Real-time Scan Settings*** (Scaninstellingen > Realtimescaninstellingen). Het scherm ***Real-time Scan Settings*** (Realtimescaninstellingen) verschijnt.

14. Klik op het tab ***Target*** (Doel) en kies alleen de volgende opties, de overige opties schakelt u uit:

   - ***Real-Time Scan Settings (Realtimescaninstellingen) > Enable virus/malware scan (Activeer virus/malwarescan).***

- ***Real-Time Scan Settings (Realtimescaninstellingen)> Enable spyware/grayware scan (Activeer spyware/graywarescan).***
- ***Files to Scan (Te scannen bestanden) > File types scanned by IntelliScan (Bestandstypen gescand door IntelliScan).***
- ***Scan Settings (Scaninstellingen) > Scan compressed files (Scan de gecomprimeerde bestanden).***
- ***Scan Settings (Scaninstellingen) > Scan OLE objects (OLE-objecten scannen).***
- ***Virus/Malware Scan Settings only (Alleen scaninstellingen voor virussen/malware) > Enable IntelliTrap (IntelliTrap inschakelen).***

15. Klik op de tab Scan Exclusion (Scanuitsluiting) en kies alleen de volgende opties, schakel de overige opties uit:

    - ***Scan Exclusion (Scanuitsluiting) > Enable scan exclusion (Scanuitsluiting inschakelen).***
    - ***Scan Exclusion (Scanuitsluiting) > Apply scan exclusion settings to all scan types (Instellingen voor uitsluitingen toepassen op alle scantypen).***
    - ***Scan Exclusion List (Directories) (Uitsluitingslijst [mappen]) > Exclude directories where Trend Micro products are installed (Mappen uitsluiten waarin Trend Micro-producten zijn geïnstalleerd).***
    - Zorg ervoor dat ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies*** en de mappen ***E:*** en ***G:*** zijn opgenomen in de ***Exclusion List*** (Uitsluitingslijst).

16. Klik op de tab ***Action*** (Actie).

17. Laat de standaardinstellingen staan en schakel de volgende opties uit:

    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected (Plaats op eindpunten een melding wanneer virus/malware is gedetecteerd).***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected (Plaats op eindpunten een melding wanneer spyware/grayware is gedetecteerd).***

18. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).

19. Klik op ***Close*** (Sluiten) om het scherm ***Real-time Scan Settings*** (Realtimescaninstellingen) te sluiten.

20. Kies boven in het scherm ***Agents > Agent Management*** (Agentenbeheer).

21. Kies op de linkerzijde van het scherm ***OfficeScan Server***.

22. Kies uit de opties in ***Settings*** (Instellingen) ***Scan Settings > Scheduled Scan Settings*** (Scaninstellingen > Instellingen voor ingeplande scans). Het scherm ***Scheduled Scan Settings*** (Instellingen voor ingeplande scans) verschijnt.

23. Klik op het tab ***Target*** (Doel) en kies alleen de volgende opties, de overige opties schakelt u uit:

    - ***Scheduled Scan Settings (Instellingen voor ingeplande scans)> Enable virus/malware scan (Activeer de virus/malwarescan).***
    - ***Scheduled Scan Settings (Instellingen voor ingeplande scans)> Enable spyware/grayware scan (Activeer de spyware/graywarescan).***

- ***Schedule (Planning) > Weekly, every Sunday, Start time (Wekelijks, elke zondag, starttijd): 00:00 uu:mm.***
- ***Files to Scan (Te scannen bestanden) > File types scanned by IntelliScan (Bestandstypen gescand door IntelliScan).***
- ***Scan Settings (Scaninstellingen) > Scan compressed files (Scan de gecomprimeerde bestanden).***
- ***Scan Settings (Scaninstellingen) > Scan OLE objects (OLE-objecten scannen).***
- ***Virus/Malware Scan Settings only (Alleen scaninstellingen voor virussen/malware) > Scan boot Area (Opstartgebied scannen).***
- ***CPU Usage (Processorgebruik) > Low (Laag).***

24. Klik op de tab Scan Exclusion (Scanuitsluiting) en kies alleen de volgende opties, schakel de overige opties uit:
    - ***Scan Exclusion (Scanuitsluiting) > Enable scan exclusion (Scanuitsluiting inschakelen).***
    - ***Scan Exclusion (Scanuitsluiting) > Apply scan exclusion settings to all scan types (Instellingen voor uitsluitingen toepassen op alle scantypen).***
    - ***Scan Exclusion List (Directories) (Uitsluitingslijst [mappen]) > Exclude directories where Trend Micro products are installed (Mappen uitsluiten waarin Trend Micro-producten zijn geïnstalleerd).***
    - Zorg ervoor dat de ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies*** en de mappen ***E:*** en ***G:*** zijn opgenomen in de uitsluitingslijst.
25. Klik op de tab ***Action*** (Actie).
26. Laat de standaardinstellingen staan en schakel de volgende opties uit:
    - ***Virus/Malware > Display a notification message on the endpoints when virus/malware is detected (Plaats op eindpunten een melding wanneer virus/malware is gedetecteerd).***
    - ***Spyware/Grayware > Display a notification message on the endpoints when spyware/grayware is detected (Plaats op eindpunten een melding wanneer spyware/grayware is gedetecteerd).***
27. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
28. Klik op ***Close*** (Sluiten) om het scherm ***Scheduled Scan Settings*** (Instellingen voor ingeplande scans) te sluiten.
29. Kies boven in het scherm ***Agents > Agent Management*** (Agentenbeheer).
30. Kies op de linkerzijde van het scherm ***OfficeScan Server***.
31. Kies uit de opties in ***Settings*** (Instellingen) ***Scan Settings > Scan Now Settings*** (Scaninstellingen > (Instellingen nu scannen). Het scherm ***Scan Now Settings*** (Instellingen nu scannen) verschijnt.
32. Klik op het tab ***Target*** (Doel) en kies alleen de volgende opties, de overige opties schakelt u uit:
    - ***Scan Now Settings (Instellingen nu scannen) > Enable virus/malware scan (Activeer de virus/malwarescan).***
    - ***Scan Now Settings (Instellingen nu scannen) > Enable spyware/grayware scan (Activeer de spyware/graywarescan).***

- ***Files to Scan (Te scannen bestanden) > File types scanned by IntelliScan (Bestandstypen gescand door IntelliScan).***
- ***Scan Settings (Scaninstellingen) > Scan compressed files (Scan de gecomprimeerde bestanden).***
- ***Scan Settings (Scaninstellingen) > Scan OLE objects (OLE-objecten scannen).***
- ***Virus/Malware Scan Settings only (Alleen scaninstellingen voor virussen/malware) > Scan boot Area (Opstartgebied scannen).***
- ***CPU Usage (Processorgebruik) > Low (Laag).***

33. Klik op de tab ***Scan Exclusion*** (Scanuitsluiting) en kies alleen de volgende opties en schakel de overige opties uit:
    - ***Scan Exclusion (Scanuitsluiting) > Enable scan exclusion (Scanuitsluiting inschakelen).***
    - ***Scan Exclusion (Scanuitsluiting) > Apply scan exclusion settings to all scan types (Instellingen voor uitsluitingen toepassen op alle scantypen).***
    - ***Scan Exclusion List (Directories) (Uitsluitingslijst [mappen]) > Exclude directories where Trend Micro products are installed (Mappen uitsluiten waarin Trend Micro-producten zijn geïnstalleerd).***
    - Zorg dat de ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** en ***G:***
34. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
35. Klik op ***Close*** (Sluiten) om het scherm ***Scan Now Settings*** (Instellingen nu scannen) te sluiten.
36. Kies boven in het scherm ***Agents > Agent Management*** (Agentenbeheer).
37. Kies op de linkerzijde van het scherm ***OfficeScan Server***.
38. Selecteer uit de opties ***Settings*** (Instellingen) ***Web Reputation Settings*** (Webreputatie-instellingen). Het scherm ***Web Reputation Settings*** (Webreputatie-instellingen) verschijnt.
39. Klik op de tab ***External Clients*** (Externe clients) en schakel ***Enable Web reputation policy on the following operating systems*** (Activeer webreputatieregels op de volgende systemen) uit, indien deze tijdens de installatie is geactiveerd.
40. Klik op de tab ***Internal Agents*** (Interne agenten) en deselecteer ***Enable Web reputation policy on the following operating systems*** (Activeer webreputatieregels op de volgende besturingssystemen), indien deze tijdens de installatie is geselecteerd.
41. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
42. Klik op ***Close*** (Sluiten) om het scherm ***Web Reputation*** (Webreputatie) te sluiten.
43. Kies boven in het scherm ***Agents > Agent Management*** (Agentenbeheer).
44. Kies op de linkerzijde van het scherm ***OfficeScan Server***.
45. Kies uit de opties in ***Settings*** (Instellingen) ***Behavior Monitoring Settings*** (Instellingen voor bewaking van gedrag). Het scherm ***Behavior Monitoring Settings*** (Instellingen voor bewaking van gedrag) verschijnt.
46. Schakel de opties ***Enable Malware Behavior Blocking*** (Activeer blokkeren malwaregedrag) en ***Enable Event Monitoring*** (Activeer bewaking van gebeurtenissen) uit.
47. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).

48. Klik op ***Close*** (Sluiten) om het scherm ***Behavior Monitoring*** (Bewaking van gedrag) te sluiten.
49. Kies boven in het scherm ***Agents > Agent Management*** (Agentenbeheer).
50. Kies op de linkerzijde van het scherm ***OfficeScan Server***.
51. Kies uit de opties in ***Settings*** (Instellingen) ***Device Control Settings*** (Instellingen voor apparaatcontrole). Het scherm ***Device Control Settings*** (Instellingen voor apparaatcontrole) verschijnt.
52. Klik op de tab ***External Agents*** (Externe agenten) en deselecteer de volgende opties:
    - ***Notification (Melding) > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Laat een melding op eindpunten zien wanneer OfficeScan ongeautoriseerde toegang detecteert).***
    - ***Blokkeer de functie AutoRun op USB-opslagapparaten.***
    - ***Activeer Device Control (Apparaatcontrole).***
53. Klik op de tab ***Internal Agents*** (Interne agenten) en deselecteer de volgende opties:
    - ***Notification (Melding) > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Laat een melding op eindpunten zien wanneer OfficeScan ongeautoriseerde toegang detecteert).***
    - ***Blokkeer de functie AutoRun op USB-opslagapparaten.***
    - ***Activeer Device Control (Apparaatcontrole).***
54. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
55. Klik op ***Close*** (Sluiten) om het scherm ***Device Control Settings*** (Instellingen apparaatcontrole) te sluiten.
56. Kies opnieuw uit de ***Settings*** (Instellingen) opties ***Device Control Settings*** (Instellingen apparaatcontrole). Het scherm ***Device Control Settings*** (Instellingen voor apparaatcontrole) verschijnt.
57. Klik op de tab ***External Agents*** (Externe agenten) en deselecteer ***Enable Device Control*** (Activeer apparaatcontrole).
58. Klik op de tab ***Internal Agents*** (Interne agenten) en deselecteer ***Enable Device Control*** (Activeer apparaatcontrole).
59. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
60. Klik op ***Close*** (Sluiten) om het scherm ***Device Control Settings*** (Instellingen apparaatcontrole) te sluiten.
61. Kies op de linkerzijde van het scherm ***Agents > Agent Management*** (Agentenbeheer).
62. Kies op de linkerzijde van het scherm ***OfficeScan Server***.
63. Kies uit de opties in ***Settings*** (Instellingen) ***Privileges and Other Settings*** (Bevoegdheden en andere instellingen).
64. Klik op de tab ***Privileges*** (Bevoegdheden) en kies alleen de volgende opties, schakel de overige opties uit:
    - ***Scan Privileges (Scanbevoegdheden) > Configure Manual Scan Settings (Instellingen voor handmatig scannen configureren).***

- ***Scan Privileges (Scanbevoegdheden) > Configure Real-time Scan Settings (Instellingen voor realtimescannen configureren).***
- ***Scan Privileges (Scanbevoegdheden) > Configure Scheduled Scan Settings (Instellingen voor gepland scannen configureren).***
- ***Proxy Setting Privileges (Bevoegdheden voor proxy-instellingen) > Allow the agent user to configure proxy settings (De agentgebruiker kan proxy-instellingen configureren).***
- ***Uninstallation (deïnstallatie) > wachtwoord vereist.*** Voer een bruikbaar wachtwoord in en bevestig dit.
- ***Unload and Unlock (Leegmaken en ontgrendelen) > Wachtwoord vereist.*** Voer een bruikbaar wachtwoord in en bevestig dit.

65. Klik op de tab ***Other Settings*** (Overige instellingen).
66. Deselecteer alle opties.

OPMERKING: Het is belangrijk om de volgende opties uit te schakelen.

- ***OfficeScan Agent Self-protection (Zelfbecherming agent OfficeScan) > Protect OfficeScan agent services (Bescherm OfficeScan-agentservices).***
- ***OfficeScan Agent Self-protection (Zelfbecherming agent OfficeScan)> Protect files in the OfficeScan agent installation folder (Bescherm bestanden in de OfficeScan-agentinstallatiemap).***
- ***OfficeScan Agent Self-protection (Zelfbecherming agent OfficeScan)> Protect OfficeScan agent registry keys (Bescherm de OfficeScan-agentregistratienummers).***
- ***OfficeScan Agent Self-protection (Zelfbeveiliging OfficeScan-agent)> Protect OfficeScan agent processes (Bescherm de OfficeScan-agentprocessen).***

67. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
68. Klik op ***Close*** (Sluiten) om het scherm ***Privileges and Other Settings*** (Bevoegdheden en andere instellingen) te sluiten.
69. Kies boven in het scherm ***Agents > Agent Management*** (Agentbeheer).
70. Kies op de linkerzijde van het scherm ***OfficeScan Server***.
71. Kies uit de opties in ***Settings*** (Instellingen) ***Additional Service Settings*** (Aanvullende service-instellingen).
72. Schakel de optie ***Enable service on the following operating systems*** (Activeer service op de volgende systemen) uit.
73. Klik op ***Apply to All Agents*** (Toepassen op alle agenten).
74. Klik op ***Close*** (Sluiten) om het scherm ***Additional Service Settings*** (Aanvullende service-instellingen) te sluiten.
75. Kies boven in het scherm ***Agents > Global Agent Settings*** (Algemene agentinstellingen).
76. Kies alleen de volgende opties en schakel de overige opties uit:

- ***Scan Settings for Large Compressed Files > Do not scan files in the compressed file if the size exceeds 2 MB*** (Scaninstellingen voor grote gecomprimeerde bestanden > Gecomprimeerde bestanden die groter zijn dan 2 MB, niet scannen). ***Real-Time Scan*** en ***Manual Scan/Schedule Scan/Scan Now*** (Handmatige scan/Geplande scan en Nu scannen).

- ***Scan Settings for Large Compressed Files (Scaninstellingen voor grote gecomprimeerde bestanden) > In a compressed file scan only the first 100 files (In een gecomprimeerd bestand alleen de eerste 100 bestanden scannen). Real-Time Scan*** en ***Manual Scan/Schedule Scan/Scan Now*** (Handmatige scan/Geplande scan en Nu scannen).
- ***Scan Settings (Scaninstellingen) > Exclude the OfficeScan server database folder from Real-time Scan (Map met OfficeScan-serverdatabase uitsluiten van realtimescan).***
- ***Scan Settings (Scaninstellingen) > Exclude Microsoft Exchange server folders and files from scans (Mappen van Microsoft Exchange-server uitsluiten van scan).***

77. Klik op ***Save*** (Opslaan).
78. Kies boven in het scherm ***Updates > Agents > Manual Updates*** (Handmatige updates).
79. Selecteer ***Manually select agents*** (Agenten handmatig selecteren) en klik op ***Select*** (Selecteer).
80. Dubbelklik op de gewenste domeinnaam onder ***OfficeScan Server***.
81. Selecteer een voor een de clientsystemen en klik op ***Initiate Update*** (Start update).
82. Klik ***OK*** in het berichtenvak.
83. Klik op ***Log off*** (Afmelden) en sluit de OfficeScan Web Console.

Installatierichtlijnen voor Trend Micro OfficeScan Post

1. Schakel de Loopback-verbinding in. Raadpleeg Schakel de Loopback-verbinding in op pagina 6 voor meer informatie.
2. Configureer de Computerbrowserservice. Raadpleeg Computerbrowserservice configureren na installatie van de antivirussoftware op pagina 7 voor meer informatie.

Troubleshooting Domains of Systems Not Listed (Probleemoplossingsdomeinen of niet genoemde systemen) in het scherm Domains and Endpoints (Domeinen en eindpunten)

Tijdens de geprefereerde push-installatieprocedures van Trend Micro OfficeScan Client/Server Edition 11.0 SP1 en Trend Micro OfficeScan Client/Server Edition XG 12.0 moeten de domeinen en systemen vermeld staan voor het pushen van installatie op het systeem. Tijdens deze stappen krijgt u twee opties om de antivirussoftware op de clientsystemen (Acquisition, Review and INW) te installeren.

Zie Trend Micro OfficeScan - Nieuwe installatieprocedure (geprefereerde push-installatiemethode voor 11.0 SP1) op pagina 58 voor 11.0 SP1.
Zie Trend Micro OfficeScan - Nieuwe installatieprocedure (geprefereerde push-installatiemethode voor 12.0) op pagina 69 voor 12.0.

1. Gebruik de IP-adressen van de clientapparaten (Acquisition, Review en INW) op de managementconsole en doe het volgende:
   a. Zet de IP van elk clientsysteem een voor een in het vak ***Search for endpoints*** (Zoek naar eindpunten) en druk op ***Enter***.

b. Voer het ***<domeinnaam>\gebruikersnaam*** en wachtwoord in en klik op ***Log on*** (Aanmelden).

c. Kies één van de volgende stappen op basis van uw versie van Trend Micro:

i. Ga terug naar stap 10 op pagina 59 voor 11.0 SP1.

ii. Ga terug naar stap 10 op pagina 70 voor 12.0.

2. Als u de IP-adressen van de systemen niet kent, of als de vorige optie niet werkt, ga dan naar ieder clientapparaat (Acquisition, Review en INW Server) en doe het volgende:

a. Meld u aan als **Administrator** of als lid van die groep op alle clientapparaten.

b. Klik op ***Start > Run*** (Start > Uitvoeren).

c. Typ ***<Anti-Virus Management Console_server_IP_address>*** en druk op ***Enter***. Desgevraagd voert u gebruikersnaam en wachtwoord in.

d. Ga naar ***<Anti-Virus Management Console_server_IP _address>\ofsscan*** en dubbelklik op ***AutoPcc.exe***. Desgevraagd voert u gebruikersnaam en wachtwoord in.

e. Herstart de clientsystemen nadat de installatie is afgerond.

f. Meld u aan als **Administrator** of als een lid van die groep op alle clientapparaten en wacht totdat het Trend Micro OfficeScan-pictogram in het systeemvak blauw is geworden.

g. Kies één van de volgende stappen op basis van uw versie van Trend Micro:

i. Zie Serverconfiguratie Trend Micro OfficeScan Console voor 11.0 SP1 op pagina 59 voor 11.0 SP1.

ii. Zie Serverconfiguratie Trend Micro OfficeScan Console voor 12.0 op pagina 70 voor 12.0.