Istruzioni per l'installazione di Mac-Lab/ CardioLab Anti-Virus (IT)

Software Mac-Lab/CardioLab versione 6.9.6

Introduzione

Il software antivirus aiuta le strutture a rispettare le norme sulla privacy, come la legge HIPAA (Legge sulla trasferibilità e gli obblighi di rendere conto in materia di copertura assicurativa sanitaria).

Utilizzo del documento

Utilizzare il presente documento per installare il software antivirus convalidato per il sistema Mac-Lab/CardioLab v6.9.6.

Cronologia delle revisioni

Revisione	Data	Commenti
A	16 febbraio 2016	Versione pubblica iniziale.
B	9 giugno 2016	Aggiornamento di Trend Micro per il supporto CO_2.
C	16 maggio 2017	Aggiornamenti di McAfee ePolicy Orchestrator, Trend Micro e Symantec.
D	10 luglio 2017	Aggiornamenti per 12.1.6 MP5, Trend Micro 11.0 SP1, McAfee ePO 5.9 e McAfee VSE 8.8 Patch 9.
E	14 agosto 2017	Rimozione dei riferimenti a McAfee ePolicy Orchestrator 5.9 e McAfee VirusScan Enterprise 8.8 Patch 9. Aggiunta lingue UI 6.9.6 R3.
F	25 settembre 2017	Aggiunti McAfee ePO 5.9 e McAfee VSE 8.8 Patch 9. Collegamenti aggiornati per Trend Micro 11 e 12.

Guida introduttiva

Requisiti del software antivirus

AVVERTENZA: INSTALLAZIONE DI PROGRAMMI ANTIVIRUS RICHIESTA

Il sistema viene fornito senza alcuna protezione antivirus. Prima di collegare il sistema a una qualsiasi rete, assicurarsi che vi sia installato un antivirus convalidato. La mancanza di una protezione dai virus valida potrebbe portare all'instabilità o al guasto del sistema.

Tenere conto dei seguenti requisiti:

- Il software antivirus non viene fornito con il sistema Mac-Lab/CardioLab; spetta al cliente procurarselo, installarlo e mantenerlo in condizioni di funzionamento,
- nonché aggiornarne i file di definizione antivirus.
- In caso di rilevamento di un virus sul sistema, contattare l'amministratore del sistema ed il servizio di assistenza tecnica della GE.
- Installare solo i pacchetti software antivirus elencati nella sezione Software antivirus convalidati.
- Accedere come amministratore o come membro di tale gruppo per eseguire le attività indicate in questo documento.
- La lingua del programma antivirus convalidato deve corrispondere a quella del sistema operativo, se possibile. Nel caso in cui non esistano programmi antivirus convalidati con la lingua corrispondente a quella del sistema, installare la versione del software antivirus in inglese.

Programmi antivirus convalidati

AVVERTENZA: INSTABILITÀ DEL SISTEMA

Non installare né utilizzare antivirus non convalidati (comprese eventuali versioni non convalidate). Ciò potrebbe provocare l'instabilità o il guasto del sistema. Usare esclusivamente programmi antivirus convalidati, nella lingua appropriata.

NOTA: Se non è disponibile un software antivirus nella lingua specifica utilizzata per il sistema operativo, installare la versione del software antivirus in inglese.

I sistemi Mac-Lab/CardioLab versione 6.9.6 sono stati convalidati per l'utilizzo dei software antivirus elencati nella tabella seguente.

Programmi antivirus supportati	Lingue supportate da MLCL	Versioni supportate del programma antivirus
McAfee VirusScan Enterprise	Inglese, francese, tedesco, italiano, spagnolo, svedese, norvegese, danese, olandese, cinese, giapponese	8.8 Patch 3 8.8 Patch 4 8.8 Patch 8 8.8 Patch 9
McAfee ePolicy Orchestrator (con McAfee VirusScan Enterprise)	Inglese, francese, tedesco, italiano, spagnolo, svedese, norvegese, danese, olandese, cinese, giapponese	v5.0 v5.3.2 v5.9
Symantec EndPoint Protection	Inglese, francese, tedesco, italiano, spagnolo, svedese, norvegese, danese, olandese, cinese, giapponese	12.1.2, 12.1.6 MP5, 14.0 MP1
Trend Micro OfficeScan Client/Server Edition	Inglese, francese, tedesco, italiano, spagnolo, svedese, norvegese, danese, olandese, cinese, giapponese	10.6 SP2, 11.0 SP1, XG 12.0

Il software antivirus supportato è disponibile nelle lingue elencate nella tabella seguente.

Versione di MLCL	Lingue supportate da MLCL
M6.9.6 R1	Inglese
M6.9.6 R2	Inglese, francese, tedesco
M6.9.6 R3	Inglese, francese, tedesco, italiano, spagnolo, svedese, norvegese, danese, olandese, cinese, giapponese

Configurazione del server della console di gestione antivirus

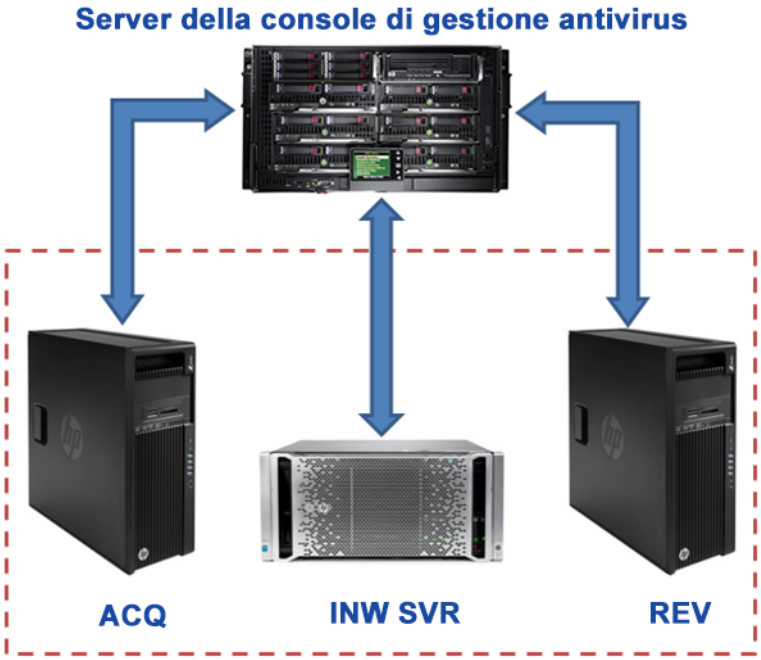
La console di gestione antivirus deve essere installata sul server della console di gestione antivirus.

La comunicazione tra il server della console di gestione antivirus e i dispositivi Mac-Lab/CardioLab può avvenire in vari modi, a seconda dell'ambiente:

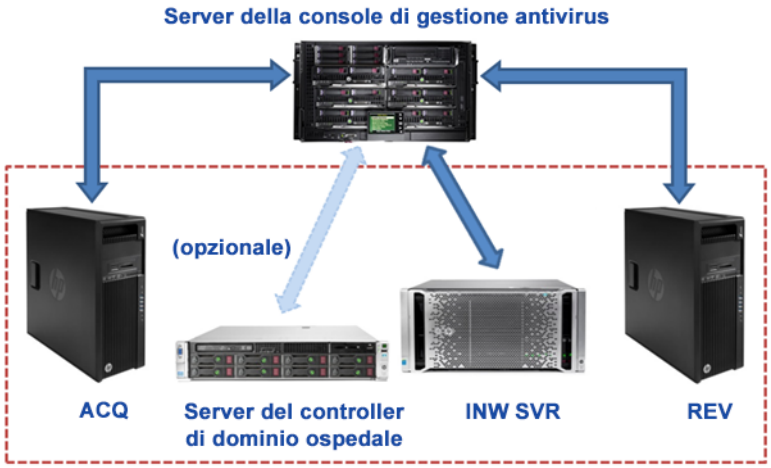
1. Ambiente controller di dominio INW - Server della console di gestione antivirus non incluso nel dominio server INW
   - Tipo di comunicazione - 1 <stessa rete con stessa subnet mask>
   - Tipo di comunicazione - 2 <rete diversa con subnet mask diversa>
2. Ambiente controller di dominio ospedale - Server della console di gestione antivirus non incluso nel dominio controller di dominio ospedale
   - Tipo di comunicazione - 1 <rete diversa con subnet mask diversa>
3. Ambiente controller di dominio ospedale - Server della console di gestione antivirus nel dominio controller di dominio ospedale
   - Tipo di comunicazione - 1 <stessa rete con stessa subnet mask>

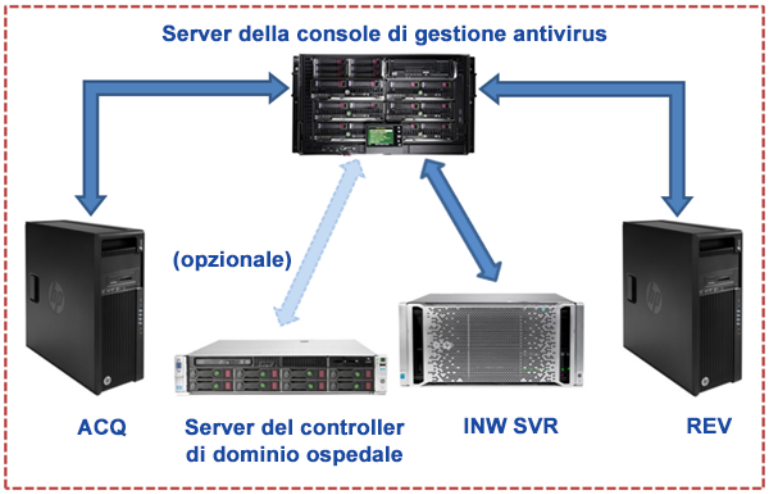
NOTA: Il server della console di gestione antivirus deve essere dotato di due porte di rete. Una porta di rete per la connessione alla rete Centricity Cardiology INW e una seconda porta di rete per la connessione alla rete ospedaliera.

Schema a blocchi dell'ambiente controller di dominio INW



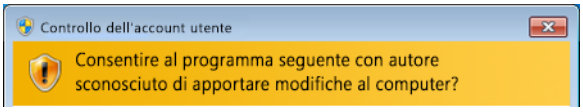
Schema a blocchi dell'ambiente controller di dominio ospedale





Controllo account utente

Controllo account utente è una funzione di Windows che impedisce di apportare modifiche non autorizzate a un computer. Nel corso di alcune procedure descritte nel presente manuale, viene visualizzato un messaggio del Controllo account utente.



Se il messaggio viene visualizzato dopo l'esecuzione delle procedure descritte in questo manuale, è possibile continuare tranquillamente.

Istruzioni per l'installazione dell'antivirus

Fare clic sul software antivirus che si desidera installare:

Procedure comuni per l'installazione dei software antivirus

Utilizzare le procedure descritte in questa sezione quando indicato dalle istruzioni per l'installazione del software antivirus.

Disattivazione di Loopback Connection (Connessione loopback)

In un sistema di acquisizione connesso all'ambiente Mac-Lab/CardioLab, disabilitare Loopback Connection (Connessione loopback) per rilevare tutti i sistemi client presenti nel dominio che condividono la stessa subnet mask.

1. Accedere come **Administrator (Amministratore)** o come membro di tale gruppo.
2. Fare clic con il pulsante destro del mouse su ***Network (Rete)*** sul desktop e selezionare ***Properties (Proprietà)***.
3. Fare clic su ***Change adapter settings (Modifica impostazioni scheda).***
4. Fare clic con il pulsante destro del mouse su ***Loopback Connection (Connessione loopback)*** e selezionare ***Disable (Disattiva)***.
5. Riavviare il sistema di acquisizione.

NOTA: La disattivazione della connessione loopback sul sistema di acquisizione è necessaria per il rilevamento di tutti i sistemi client con la stessa subnet mask nel dominio.

Attivazione di Loopback Connection (Connessione loopback)

Nei sistemi di acquisizione connessi all'ambiente Mac-Lab/CardioLab, attivare Loopback Connection (Connessione loopback) procedendo come segue.

1. Accedere come **Administrator (Amministratore)** o come membro di tale gruppo.
2. Fare clic con il pulsante destro del mouse su ***Network (Rete)*** sul desktop e selezionare ***Properties (Proprietà)***.
3. Fare clic su ***Change adapter settings (Modifica impostazioni scheda)***.
4. Fare clic con il pulsante destro del mouse su ***Loopback Connection (Connessione loopback)*** e selezionare ***Enable (Attiva)***.
5. Riavviare il sistema di acquisizione.

Configurazione del servizio Browser di computer prima dell'installazione dell'antivirus

Controllare che l'impostazione del servizio Browser di computer nei sistemi di acquisizione e revisione collegati in rete sia configurata correttamente.

1. Fare clic su ***Start > Control Panel (Pannello di controllo) > Network and Sharing Center (Centro connessioni di rete e condivisione)***.
2. Fare clic su ***Change advanced sharing settings (Modifica impostazioni di condivisione avanzate)***.
3. Espandere ***Home or Work (Casa o Ufficio)***.
4. Controllare che l'opzione ***Turn on file and printer sharing (Attiva condivisione file e stampanti)*** sia selezionata.
5. Fare clic su ***Save changes (Salva modifiche)***.
6. Fare clic su ***Start > Run (Esegui)***.
7. Digitare **services.msc** e premere **Invio**.
8. Fare doppio clic sul servizio ***Computer Browser (Browser di computer)***.
9. Controllare che l'opzione ***Startup type (Tipo di avvio)*** sia impostata su ***Automatic (Automatico)*****.** In caso contrario, modificare l'impostazione e fare clic su ***Start (Avvia)***.
10. Fare clic su ***OK***.
11. Chiudere la finestra ***Services (Servizi)***.

Configurazione del servizio Browser di computer dopo l'installazione dell'antivirus

Dopo aver installato il software antivirus, controllare che l'impostazione del servizio Browser di computer nei sistemi di acquisizione e revisione collegati in rete sia configurata correttamente.

1. Fare clic su ***Start > Run (Esegui)***.
2. Digitare **services.msc** e premere **Invio**.
3. Fare doppio clic sul servizio ***Computer Browser (Browser di computer)***.
4. Impostare ***Startup type (Tipo di avvio)*** su ***Manual (Manuale)***.
5. Fare clic su ***OK***.
6. Chiudere la finestra ***Services (Servizi)***.

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

Panoramica dell'installazione

Installare Symantec EndPoint Protection solo in ambienti Mac-Lab/CardioLab collegati in rete. In un ambiente di rete, il software Symantec EndPoint Protection deve essere installato sul server della console di gestione antivirus e distribuito nel server Centricity Cardiology INW e nelle workstation di acquisizione/revisione come client. Attenersi alle seguenti istruzioni per installare e configurare ***Symantec EndPoint Protection***.

La responsabilità degli aggiornamenti antivirus spetta all'ospedale. Aggiornare regolarmente le definizioni, per assicurare che il sistema sia sempre protetto dai virus più recenti.

Linee guida da seguire prima dell'installazione

1. Per il corretto funzionamento, la console di gestione antivirus Symantec deve essere installata attenendosi alle istruzioni fornite da Symantec.
2. Accedere come **Administrator (Amministratore)** o come membro di tale gruppo in tutti i sistemi client (acquisizione, revisione e server INW) per installare il software antivirus.
3. Aprire il prompt dei comandi in modalità ***Run As Administrator (Esegui come amministratore)***.
4. Accedere a C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

NOTA: Per configurare il server INW, accedere a C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Digitare **UpdateRegSymantec.ps1** e premere ***Invio***.
6. Accertarsi che lo script sia stato eseguito correttamente.

   Se il percorso della cartella suindicato non è presente, effettuare le seguenti operazioni per tutti i sistemi MLCL, ad eccezione del server INW di MLCL 6.9.6R1 (sistema operativo del server: Windows Server 2008 R2).

   a. Fare clic sul pulsante ***Start*** e scegliere ***Run (Esegui)***.

   b. Digitare **Regedit.exe** e fare clic su ***OK***.

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

   d. Individuare il registro ***State (Stato)*** e fare doppio clic.

   e. Impostare ***Base*** su ***Decimal (Decimale)***.

   f. Impostare ***Value data (Dati valore)*** su ***146432***.

   g. Fare clic su ***OK*** per chiudere il registro.

7. Disattivare Loopback Connection (Connessione loopback). Per ulteriori informazioni, consultare Disattivazione di Loopback Connection (Connessione loopback) a pagina 6.

8. Configurare il servizio Browser di computer. Per ulteriori informazioni, consultare Configurazione del servizio Browser di computer prima dell'installazione dell'antivirus a pagina 7.

Symantec EndPoint Protection - Procedura di distribuzione di una nuova installazione (metodo di installazione push preferito)

1. Fare clic su ***Start > All Programs (Tutti i programmi) > Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager***.
2. Inserire nome utente e password per accedere a Symantec Endpoint Protection Manager. Se viene visualizzata una richiesta di protezione, fare clic su ***Yes (Sì)***.
3. Selezionare ***Do not show this Welcome Page again (Non visualizzare più questa pagina di benvenuto)*** e fare clic su click ***Close (Chiudi)*** per chiudere la schermata di benvenuto.

NOTA: Per la versione 14.0 MP1, fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Getting Started on Symantec EndPoint Protection (Introduzione a Symantec EndPoint Protection)***.

4. Fare clic su ***Admin (Amministratore)*** nella finestra ***Symantec EndPoint Protection Manager***.
5. Fare clic su ***Install Packages (Installa pacchetti)*** nel riquadro inferiore.
6. Fare clic su ***Client Install Feature Set (Insieme di funzioni di installazione client)*** nel riquadro superiore.
7. Fare clic con il pulsante destro del mouse sulla finestra ***Client Install Feature Set (Insieme di funzioni di installazione client)*** e selezionare ***Add (Aggiungi)***. Viene visualizzata la finestra Add Client Install Feature Set (Aggiungi insieme di funzioni di installazione client).
8. Immettere il nome corretto e registrarlo perché sarà necessario in un secondo momento.
9. Accertarsi che ***Feature set version (Versione insieme di funzioni)*** sia ***12.1 RU2 and later (12.1 RU2 e successive)***.
10. Selezionare solo le seguenti funzioni e deselezionare le altre.
    - ***Virus, Spyware e Basic Download Protection (Protezione da virus, spyware e download base)***.
    - ***Advanced Download Protection (Protezione download avanzata)*.**
11. Nella finestra del messaggio fare clic su ***OK***.
12. Solo per le versioni 12.1.2 e 12.1.6 MP5, fare clic su ***OK*** per chiudere la finestra ***Add Client Install Feature Set (Aggiungi insieme di funzioni di installazione client)***.
13. Fare clic su ***Home (Inizio)*** nella finestra ***Symantec Endpoint Protection Manager.***
14. A seconda della versione del software, procedere come segue:
    - **Versioni 12.1.2 e 12.1.6 MP5:** Selezionare ***Install protection client to computers (Installa client di protezione sui computer)*** dall'elenco a discesa ***Common Tasks (Attività comuni)*** nell'angolo superiore destro della finestra ***Home (Inizio)***. Viene visualizzata la schermata Client Deployment Type (Tipo di distribuzione client).
    - **Versione 14.0 MP1:** Fare clic su ***Clients (Client)*** nella finestra ***Symantec Endpoint Protection Manager***. Fare clic su ***Install a client (Installa un client)*** in ***Tasks (Attività)***.

Viene visualizzata la schermata ***Client Deployment wizard (Distribuzione guidata client)***.

15. Selezionare ***New Package Deployment (Distribuzione nuovo pacchetto)*** e fare clic su ***Next (Avanti)***.

16. Selezionare il nome dell'insieme di funzioni creato al passaggio 8. Mantenere le impostazioni predefinite di tutte le altre voci e fare clic su ***Next (Avanti)***.

NOTA: Per la versione 14.1 MP1, in ***Scheduled Scans (Scansioni programmate)*** deselezionare ***Delay scheduled scans when running on batteries (Ritarda scansioni programmate se il sistema funziona a batterie) e Allow user-defined scheduled scans to run when scan author is not logged on (Consenti l'esecuzione di scansioni programmate definite dall'utente quando l'autore della scansione non è collegato)***.

17. Selezionare ***Remote push (Push remoto)*** e fare clic su ***Next (Avanti)***. Attendere che venga visualizzata la schermata ***Computer selection (Selezione computer)***.

18. Espandere ***<Domain> (<Dominio>)*** (ad esempio: INW). I sistemi connessi al dominio vengono visualizzati nella finestra ***Computer selection (Selezione computer)***.

NOTA: Se non vengono riconosciuti tutti i sistemi, fare clic su ***Search Network (Cerca nella rete)*** e scegliere ***Find Computers (Trova computer)***. Utilizzare il metodo di rilevamento ***search by IP address (cerca per indirizzo IP)*** per identificare i sistemi client (acquisizione, revisione e server INW).

19. Selezionare tutte le macchine client Mac-Lab/CardioLab connesse al dominio e fare clic su **>>**. Viene visualizzata la finestra ***Login Credentials (Credenziali di accesso)***.

20. Immettere nome utente, password e nome del dominio/computer e fare clic su ***OK***.

21. Accertarsi che tutte le macchine selezionate appaiano in ***Install Protection Client (Installa client di protezione)*** e fare clic su ***Next (Avanti)***.

22. Fare clic su ***Send (Invia)*** e attendere che il software antivirus Symantec venga distribuito su tutti i sistemi client (acquisizione, revisione e server INW). Al termine dell'operazione, viene visualizzata la schermata ***Deployment Summary (Riepilogo distribuzione)***.

23. Fare clic su ***Next (Avanti)*** e quindi su ***Finish (Fine)*** per completare Client Deployment Wizard (Distribuzione guidata client).

24. Attendere che l'icona Symantec venga visualizzata nella barra delle applicazioni e riavviare tutte le macchine client (acquisizione, revisione e server INW). Dopo il riavvio, accedere come Administrator (Amministratore) o come membro di tale gruppo su tutte le macchine client.

Configurazioni della console del server di Symantec EndPoint Protection

1. Selezionare ***Start > All Programs (Tutti i programmi) > Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager***. Viene visualizzata la finestra di accesso a Symantec EndPoint Protection Manager.

2. Immettere la password di Symantec Endpoint Protection Manager Console e fare clic su ***Log On (Accedi)***.

3. Selezionare la scheda ***Policies (Criteri)*** e fare clic su ***Virus and Spyware Protection (Protezione da virus e spyware)*** in ***Policies (Criteri)***. Viene visualizzata la finestra ***Virus and Spyware Protection Policies (Criteri di protezione da virus e spyware)***.

4. Fare clic sul criterio ***Add a Virus and Spyware Protection (Aggiungi protezione da virus e spyware)*** in ***Tasks (Attività)*****.** Viene visualizzata la finestra ***Virus and Spyware Protection (Protezione da virus e spyware)***.

5. In ***Windows Settings (Impostazioni di Windows) > Scheduled Scans (Scansioni programmate)***, fare clic su ***Administrator-Defined Scans (Scansioni definite dall'amministratore)***.

6. Selezionare ***Daily Scheduled Scan (Scansione programmata giornaliera)*** e fare clic su ***Edit (Modifica)***. Viene visualizzata la finestra ***Edit Scheduled Scan (Modifica scansione programmate)***.

7. Modificare il nome e la descrizione rispettivamente in ***Weekly Scheduled Scan (Scansione programmata settimanale)*** e ***Weekly Scan at 00:00 (Scansione settimanale alle 00:00)***.

8. Impostare ***Scan type (Tipo di scansione)*** su ***Full Scan (Scansione completa)***.

9. Selezionare la scheda ***Schedule (Programmazione)***.

10. In ***Scanning Schedule (Programmazione scansione)***, selezionare ***Weekly (Settimanale)*** e cambiare l'ora in ***00:00***.

11. In ***Scan Duration (Durata scansione)*** deselezionare ***Randomize scan start time within this period (Ora di avvio scansione casuale in questo periodo), opzione consigliata nelle VM*** e selezionare ***Scan until finished (Esegui scansione fino alla fine), opzione consigliata per ottimizzare le prestazioni della scansione***.

12. In ***Missed scheduled Scans (Scansioni programmate non eseguite)***, deselezionare ***Retry the scan within (Ritenta scansione entro)***.

13. Selezionare la scheda ***Notifications (Notifiche)*****.**

14. Deselezionare ***Display a notification message on the infected computer (Visualizza un messaggio sul computer infetto)*** e fare clic su ***OK***.

15. Selezionare la scheda ***Advanced (Avanzate)*** nella finestra the ***Administrator-Defined Scans (Scansioni definite dall'amministratore***.

16. In ***Scheduled Scans (Scansioni programmate)***, deselezionare ***Delay scheduled scans when running on batteries (Ritarda scansioni quando il sistema funziona a batterie)***, ***Allow user-defined scheduled scans to run when scan author is not logged on (Consenti esecuzione di scansioni programmate definite dall'utente quando l'autore della scansione non è collegato)*** e ***Display notifications about detections when the user logs on (Visualizza notifiche su rilevamenti quando l'utente accede)***.

NOTA: Per la versione 14.0 MP1, in ***Scheduled Scans (Scansioni programmate)*** deselezionare ***Delay scheduled scans when running on batteries (Ritarda scansioni programmate se il sistema funziona a batterie) e Allow user-defined scheduled scans to run when scan author is not logged on (Consenti l'esecuzione di scansioni programmate definite dall'utente quando l'autore della scansione non è collegato)***.

17. In ***Startup and Triggered Scans (Avvio e scansioni attivate)***, deselezionare ***Run an Active Scan when new definitions arrive (Esegui scansione attiva all'arrivo di nuove definizioni)***.

18. In ***Windows Settings (Impostazioni di Windows) > Protection Technology (Tecnologia di protezione)***, fare clic su ***Auto-Protect (Protezione automatica)***.

19. Selezionare la scheda ***Scan Details (Dettagli scansione)*** e selezionare e bloccare ***Enable Auto-Protect (Attiva protezione automatica)***.

20. Selezionare la scheda ***Notifications (Notifiche)*** e deselezionare e bloccare ***Display a notification message on the infected computer (Visualizza un messaggio di notifica sul computer infetto)*** e ***Display the Auto-Protect results dialog on the infected Computer (Visualizza risultati della protezione automatica sul computer infetto)***.

21. Selezionare la scheda ***Advanced (Avanzate)*** e in ***(Attivazione e ricaricamento protezione automatica)***, bloccare l'opzione ***When Auto-Protect is disabled, Enable after: (Quando Protezione automatica è disattivata, attivala dopo:)***.

22. In ***Additional Options (Ulteriori opzioni)*** fare clic su ***File Cache (Cache file)***.
    Si apre la finestra ***File Cache (Cache file)***.

23. Deselezionare ***Rescan cache when new definitions load (Riesegui scansione quando vengono caricate nuove definizioni)*** e fare clic su ***OK***.

24. In ***Windows Settings (Impostazioni di Windows) > Protection Technology (Tecnologia di protezione)***, fare clic su ***Download Protection (Protezione download)***.

25. Selezionare la scheda ***Notifications (Notifiche)*** e deselezionare e bloccare ***Display a notification message on the infected computer (Visualizza un messaggio di notifica sul computer infetto)***.

26. In ***Windows Settings (Impostazioni di Windows) > Protection Technology (Tecnologia di protezione)***, fare clic su ***SONAR***.

27. Selezionare la scheda ***SONAR Settings (Impostazioni SONAR)***, quindi deselezionare e bloccare ***Enable SONAR (Attiva SONAR)***.

28. In ***Windows Settings (Impostazioni di Windows) > Protection Technology (Tecnologia di protezione)*****,** fare clic su ***Early Launch Anti-Malware Driver (Avvio anticipato driver antimalware)***.

29. Deselezionare e bloccare ***Enable Symantec early launch anti-malware (Attiva avvio anticipato antimalware di Symantec)***.

30. In ***Windows Settings (Impostazioni di Windows) > Email Scans (Scansioni email)***, fare clic su ***Internet Email Auto-Protect (Protezione automatica email Internet)***.

31. Selezionare la scheda ***Scan Details (Dettagli scansione)***, quindi deselezionare e bloccare ***Enable Internet Email Auto-Protect (Attiva protezione automatica email Internet)***.

32. Selezionare la scheda ***Notifications (Notifiche)***, quindi deselezionare e bloccare ***Display a notification message on the infected computer (Visualizza un messaggio di notifica sul computer infetto)***, ***Display a progress indicator when email is being sent (Visualizza un indicatore di avanzamento quando viene inviato un messaggio email)*** e ***Display a notification area icon (Visualizza un'icona nell'area di notifica)***.

33. In ***Windows Settings (Impostazioni di Windows) > Email Scans (Scansioni email)***, fare clic su ***Microsoft Outlook Auto-Protect (Protezione automatica di Microsoft Outlook)***.

34. Seleziona la scheda ***Scan Details (Dettagli scansione)***, quindi deselezionare e bloccare ***Enable Microsoft Outlook Auto-Protect (Attiva protezione automatica di Microsoft Outlook)***.

35. Selezionare la scheda ***Notifications (Notifiche)*** e deselezionare e bloccare ***Display a notification message on the infected computer (Visualizza un messaggio di notifica sul computer infetto)***.

36. In ***Windows Settings (Impostazioni di Windows)> Email Scans (Scansioni email)***, fare clic su ***Lotus Notes Auto-Protect (Protezione automatica di Lotus Notes)*.**

37. Selezionare la scheda ***Scan Details (Scansioni email)***, quindi deselezionare e bloccare ***Enable Lotus Notes Auto-Protect (Attiva protezione automatica di Lotus Notes)***.

38. Selezionare la scheda ***Notifications (Notifiche)***, quindi deselezionare e bloccare ***Display a notification message on infected computer (Visualizza un messaggio di notifica sul computer infetto)***.

39. In ***Windows Settings (Impostazioni di Windows) > Advanced Options (Opzioni avanzate)*** , fare clic su ***Global Scan Options (Opzioni di scansione globali)***.

40. In ***Bloodhound™ Detection Settings (Impostazioni di rilevamento Bloodhound™)***, deselezionare e bloccare ***Enable Bloodhound™ heuristic virus detection (Attiv a rilevamento virus euristico Bloodhound™)***.

41. In ***Windows Settings (Impostazioni di Windows)> Advanced Options (Opzioni avanzate)***, fare clic su ***Quarantine (Quarantena)***.

42. Selezionare la scheda ***General (Generale)***, in ***When New Virus Definitions Arrive (All'arrivo di nuove definizioni virus)***, selezionare ***Do nothing (Nessuna azione)*.**

43. In ***Windows Settings (Impostazioni di Windows) > Advanced Options (Opzioni avanzate)***, fare clic su ***Miscellaneous (Varie)***.

44. Selezionare la scheda ***Notifications (Notifiche)*** e deselezionare ***Display a notification message on the client computer when definitions are outdated (Visualizza un messaggio di notifica sul computer client quando le definizioni sono obsolete)***, ***Display a notification message on the client computer when Symantec Endpoint Protection is running without virus definitions (Visualizza un messaggio di notifica sul computer client quando Symantec Endpoint Protection è in esecuzione senza definizioni virus)*** e ***Display error messages with a URL to a solution (Visualizza messaggi di errore con l'URL di una soluzione)***.

45. Fare clic su ***OK*** per chiudere la finestra dei criteri ***Virus and Spyware Protection (Protezione da virus e spyware)***.

46. Fare clic su ***Yes (Sì)*** nella finestra del messaggio ***Assign Policies (Assegna criteri)***.

47. Selezionare ***My Company (La mia azienda)*** e fare clic su ***Assign (Assegna)*.**

48. Nella finestra del messaggio fare clic su ***Yes (Sì)***.

49. In ***Policies (Criteri)*** fare clic su ***Firewall***.

50. Fare clic su ***Firewall policy (Criterio firewall)*** in ***Firewall Policies (Criteri firewall)*** e fare clic su ***Edit the policy (Modifica criterio)*** in ***Tasks (Attività)***.

51. Selezionare la scheda ***Policy Name (Nome criterio)*** e deselezionare ***Enable this policy (Attiva questo criterio)***.

52. Fare clic su ***OK***.

53. In ***Policies (Criteri)*** fare clic su ***Intrusion Prevention (Prevenzione intrusioni)***.

54. Fare clic sul criterio ***Intrusion Prevention (Prevenzione intrusioni)*** in ***Intrusion Prevention Policies (Criteri di prevenzione intrusioni)*** e fare clic su ***Edit the policy (Modifica criterio)*** in ***Tasks (Attività***).

55. Selezionare la scheda ***Policy Name (Nome criterio)*** e deselezionare ***Enable this policy (Attiva questo criterio)***.

56. A seconda della versione del software, procedere come segue:

    - **Versione 12.1.2:** Fare clic su ***Settings (Impostazioni)*** dal riquadro sinistro.
    - **Versioni 12.1.6 MP5 e 14.0 MP1:** Fare clic su ***Intrusion Prevention (Prevenzione intrusioni)*** dal riquadro sinistro.

57. Deselezionare e bloccare ***Enable Network Intrusion Prevention (Attiva prevenzione intrusioni dalla rete)*** e ***Enable Browser Intrusion Prevention for Windows (Attiva prevenzione intrusioni dal browser per Windows)***.

58. Fare clic su ***OK***.

59. In ***Policies (Criteri)*** fare clic su ***Application and Device Control (Controllo applicazioni e dispositivi)***.

60. Fare clic su ***Application and Device Control Policy (Criterio di controlli applicazioni e dispositivi)*** in ***Application and Device Control Policies (Criteri di controllo applicazioni e dispositivi)***, quindi fare clic su ***Edit the policy (Modifica criterio)*** in ***Tasks (Attività)***.

61. Selezionare la scheda ***Policy Name (Nome criterio)*** e deselezionare ***Enable this policy (Attiva questo criterio)***.

62. Fare clic su ***OK***.

63. In ***Policies (Criteri)*** fare clic su ***LiveUpdate***.

64. Selezionare ***LiveUpdate Settings policy (Criterio impostazioni LiveUpdate)*** e in ***Tasks*** (Attività) fare clic su ***Edit the policy (Modifica criterio)***.

65. In ***Overview (Panoramica) > Windows Settings (Impostazioni di Windows)*** , fare clic su ***Server Settings (Impostazioni server)***.

66. In ***Internal or External LiveUpdate Server (Server LiveUpdate interno o esterno)***, controllare che l'opzione ***Use the default management server (Usa server di gestione predefinito)*** sia selezionata e deselezionare ***Use a LiveUpdate server (Usa un server LiveUpdate)***.

67. Fare clic su ***OK***.

68. In ***Policies (Criteri)*** fare clic su ***Exceptions (Eccezioni)***.

69. Fare clic su ***Exceptions policy (Criterio eccezioni)*** e in ***Tasks (Attività)*** fare clic su ***Edit the policy (Modifica criterio)***.

70. A seconda della versione del software, procedere come segue:

    - **Versioni 12.1.2 e 12.1.6 MP5:** Fare clic su ***Exceptions (Eccezioni) > Add (Aggiungi) > Windows Exceptions (Eccezioni di Windows) > Folder (Cartella)***.
    - **Versione 14.0 MP1:** Fare clic sull'elenco a discesa ***Add (Aggiungi)*** e selezionare ***Windows Exceptions (Eccezioni di Windows) > Folder (Cartella)***.

71. Immettere i percorsi delle cartelle **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL, D:\GEData\Studies**, **E:**, **G:** uno alla volta e procedere come segue:

    a. Controllare che l'opzione ***Include subfolders (Includi sottocartelle)*** sia selezionata.

NOTA: Se viene visualizzata la finestra del messaggio ***Are you sure you want to exclude all subfolders from protection? (Escludere tutte le sottocartelle dalla protezione)***, fare clic su ***Yes (Si)***.

    b. Per ***Specify the type of scan that excludes this folder (Specifica tipo di scansione che esclude questa cartella)***, selezionare ***All (Tutti)***.

    c. Per la versione 14.0 MP1, fare clic su ***OK*** per aggiungere l'eccezione.

72. Fare clic su ***OK***.

73. Fare clic su ***Assign the policy (Assegna criterio)*** in ***Tasks (Attività)***.

74. Selezionare ***My Company (La mia azienda)*** e fare clic su ***Assign (Assegna)***.

75. Fare clic su ***Yes (Si)***.

76. Fare clic su ***Clients (Client)*** nel riquadro sinistro e selezionare la scheda ***Policies (Criteri)***.

77. In ***My Company (La mia azienda)*** selezionare ***Default Group (Gruppo predefinito)***, deselezionare ***Inherit policies and settings from parent group "My Company" (Eredita criteri e impostazioni dal gruppo padre "La mia azienda")*** e fare clic su ***Communications Settings (Impostazioni comunicazioni)*** in ***Location-Independent Policies and Settings (Criteri e Impostazioni indipendenti dalla posizione geografica)***.

NOTA: Se viene visualizzato un messaggio di avvertenza, fare clic su ***OK***, quindi fare nuovamente clic su ***Communications Settings (Impostazioni comunicazioni)*** in ***Location-Independent Policies and Settings (Criteri e impostazioni indipendenti dalla posizione geografica)***.

78. In ***Download***, accertarsi che siano selezionate le opzioni ***Download policies and content from the management server (Scarica criteri e contenuti dal server di gestione)*** e ***Push mode (Modalità push)***.

79. Fare clic su ***OK*.**

80. Fare clic su ***General Settings (Impostazioni generali)*** in ***Location-independent Policies and Settings (Criteri e impostazioni indipendenti dalla posizione geografica)***.

81. Selezionare la scheda ***Tamper Protection (Protezione da manomissioni)***, quindi deselezionare e bloccare ***Protect Symantec security software from being tampered with or shut down (Proteggi software di sicurezza Symantec da manomissioni o arresto)***.

82. Fare clic su ***OK***.

83. Fare clic su ***Admin (Amministratore)*** e selezionare ***Servers (Server)***.

84. In ***Servers (Server)***, selezionare ***Local Site (My Site) (Sito locale (Il mio sito))***.

85. In ***Tasks (Attività)***, selezionare ***Edit Site Properties (Modifica proprietà sito).***
    Si apre la finestra ***Site Properties for Locate Site (My Site) (Proprietà sito per sito localizzazione (Il mio sito))***.

86. Selezionare la scheda ***LiveUpdate*** e in ***Download Schedule (Programmazione download)*** e accertarsi che la programmazione sia impostata su ***Every 4 hour(s) (Ogni 4 ore)***.

87. Fare clic su ***OK***.

88. Fare clic su ***Log Off (Esci)*** e chiudere la console di Symantec EndPoint Protection Manager. Accertarsi che i criteri di protezione degli endpoint Symantec siano distribuiti nei sistemi client.

Linee guida da seguire dopo l'installazione di Symantec EndPoint Protection

1. Attivare Loopback Connection (Connessione loopback). Per ulteriori informazioni, consultare Attivazione di Loopback Connection (Connessione loopback) a pagina 6.

2. Configurare il servizio Browser di computer. Per ulteriori informazioni, consultare Configurazione del servizio Browser di computer dopo l'installazione dell'antivirus a pagina 7.

3. Aprire il prompt dei comandi in modalità ***Run As Administrator (Esegui come amministratore)***.

4. Accedere a C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

NOTA: Per configurare il server INW, accedere a C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Digitare **RestoreRegSymantec.ps1** e premere ***Invio***.

6. Accertarsi che lo script sia stato eseguito correttamente.
   Nota: prima di continuare, accertarsi che lo script **RestoreRegSymantec.ps1** venga eseguito correttamente.

   Se il percorso della cartella suindicato non è presente, effettuare le seguenti operazioni per tutti i sistemi MLCL, ad eccezione del server INW di MLCL 6.9.6R1 (sistema operativo del server: Windows Server 2008 R2).

   a. Fare clic sul pulsante ***Start*** e scegliere ***Run (Esegui)***.

   b. Digitare **Regedit.exe** e fare clic su ***OK***.

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

   d. Individuare il registro ***State (Stato)*** e fare doppio clic.

   e. Impostare ***Base*** su ***Decimal (Decimale)***.

   f. Impostare ***Value data (Dati valore)*** su ***65536***.

   g. Fare clic su ***OK*** per chiudere il registro.

McAfee VirusScan Enterprise

Panoramica dell'installazione

McAfee VirusScan Enterprise deve essere installato su un singolo sistema Mac-Lab/CardioLab e deve essere gestito singolarmente. Attenersi alle seguenti istruzioni per installare e configurare McAfee VirusScan Enterprise.

La responsabilità degli aggiornamenti antivirus spetta all'ospedale. Aggiornare regolarmente le definizioni, per assicurare che il sistema sia sempre protetto dai virus più recenti.

Procedura di installazione di McAfee VirusScan Enterprise

1. Accedere come **Administrator (Amministratore)** o come membro di tale gruppo.
2. Inserire il **CD McAfee VirusScan Enterprise 8.8 Patch 3**, **McAfee VirusScan Enterprise 8.8 Patch 4**, **McAfee VirusScan Enterprise 8.8 Patch 8** o **McAfee VirusScan Enterprise 8.8 Patch 9** nell'unità CD.
3. Fare doppio clic su ***SetupVSE.Exe***. Viene visualizzata la finestra di dialogo di Windows Defender.
4. Fare clic su ***Yes (Si)***. Viene visualizzata la schermata di installazione di McAfee VirusScan Enterprise.
5. Fare clic su ***Next (Avanti)***. Viene visualizzata la schermata dell'accordo di licenza dell'utente finale di McAfee.
6. Leggere l'accordo di licenza e compilare eventuali campi obbligatori. Al termine, fare clic su ***OK***. Viene visualizzata la schermata Select Setup Type (Seleziona tipo di installazione).
7. Selezionare ***Typical (Tipica)*** e fare clic su ***Next (Avanti)***. Viene visualizzata la schermata Select Access Protection Level (Seleziona livello di protezione accesso).
8. Selezionare ***Standard Protection (Protezione standard)*** e fare clic su ***Next (Avanti)***. Viene visualizzata la schermata Ready to Install (Pronto per l'installazione).
9. Fare clic su ***Install (Installa)*** e attendere che l'installazione venga completata. Al termine dell'installazione di McAfee VirusScan Enterprise, viene visualizzata la schermata ***McAfee Virus Scan Enterprise Setup has completed successfully (L'installazione di McAfee Virus Scan Enterprise è stata completata)***.
10. Deselezionare la casella di spunta ***Run On-Demand Scan (Esegui scansione a richiesta)*** e fare clic su ***Finish (Fine)***.
11. Se viene visualizzata la finestra ***Update in Progress (Aggiornamento in corso)***, fare clic su ***Cancel (Annulla)***.
12. Se viene visualizzata una finestra del messaggio con la richiesta di riavvio del sistema, fare clic su ***OK***.
13. Riavviare il sistema.
14. Accedere come **Administrator (Amministratore)** o come membro di tale gruppo.

Configurazione di McAfee VirusScan Enterprise

1. Fare clic su ***Start > All Programs (Tutti i programmi) > McAfee > VirusScan Console***. Viene visualizzata la schermata ***VirusScan Console***.
2. Fare clic con il pulsante destro del mouse su ***Access Protection (Protezione accesso)*** e selezionare ***Properties (Proprietà)***. Viene visualizzata la schermata ***Access Protection Properties (Proprietà protezione accesso)***.
3. Fare clic sulla scheda ***Access Protection (Protezione accesso)*** e deselezionare ***Enable access protection (Attiva protezione accesso)*** e ***Prevent McAfee services from being stopped (Impedisci arresto dei servizi McAfee)***.
4. Fare clic su ***OK*.**
5. Fare clic con il pulsante destro del mouse su ***Buffer Overflow Protection (Protezione da overflow del buffer)*** e selezionare ***Properties (Proprietà)***. Viene visualizzata la schermata ***Buffer Overflow Protection Properties (Proprietà protezione da overflow del buffer)***.
6. Fare clic sulla scheda ***Buffer Overflow Protection (Protezione da overflow del buffer)*** e deselezionare ***Show the messages dialog box when a buffer overflow is detected (Mostra la finestra di dialogo dei messaggi quando viene rilevato un overflow del buffer) in Buffer Overflow Settings (Impostazioni overflow del buffer)***.
7. Deselezionare ***Enable buffer overflow protection (Attiva protezione da overflow del buffer)*** in ***Buffer overflow settings (Impostazioni overflow del buffer)***.
8. Fare clic su ***OK***.
9. Fare clic con il pulsante destro del mouse su ***On-Delivery Email Scanner (Scanner email alla consegna)*** e selezionare ***Properties (Proprietà)***. Viene visualizzata la schermata ***On-Delivery Email Scanner Properties (Proprietà scanner email alla consegna)***.
10. Fare clic sulla scheda ***Scan items (Scansione elementi)*** e deselezionare le seguenti opzioni in ***Heuristics (Euristica)*:**
    - ***Find unknown program threats and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***
    - ***Find attachments with multiple extensions (Trova allegati con più estensioni).***
11. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.
12. Selezionare ***Disabled (Disattivata)*** per ***Sensitivity level (Livello di sensibilità)*** in ***Artemis (Heuristic network check for suspicious files) (Artemis (Controllo euristico rete per file sospetti))***.
13. Fare clic su ***OK***.
14. Fare clic con il pulsante destro del mouse su ***On-Delivery Email Scanner (Scanner email alla consegna)*** e selezionare ***Disable (Disattiva)***.
15. Fare clic con il pulsante desto del mouse su ***On-Access Scanner (Scanner all'accesso)*** e selezionare ***Properties (Proprietà)***. Viene visualizzata la schermata ***On-Access Scan Properties (Proprietà scansione all'accesso)***.

16. Fare clic sulla scheda ***General (Generale)*** e selezionare ***Disabled (Disattivato)*** per ***Sensitivity level (Livello di sensibilità)*** in ***Artemis (Heuristic network check for suspicious files) (Artemis (Controllo euristico rete per file sospetti))***.

17. Fare clic sulla scheda ***ScriptScan*** e deselezionare ***Enable scanning of scripts (Attiva scansione degli script)***.

18. Fare clic sulla scheda ***Blocking (Blocco)*** e deselezionare ***Block the connection when a threat is detected in a shared folder (Blocca la connessione quando viene rilevata una minaccia in una cartella condivisa)***.

19. Fare clic sulla scheda ***Messages (Messaggi)*** e deselezionare ***Show the messages dialog box when a threat is detected and display the specified text in the message (Mostra la finestra di dialogo dei messaggio quando viene rilevata una minaccia e visualizza il testo specificato nel messaggio)***.

20. Fare clic su ***All Processes (Tutti i processi)*** dal riquadro sinistro.

21. Fare clic sulla scheda ***Scan Items (Scansione elementi)*** e deselezionare le seguenti opzioni in Heuristics (Euristica).

    - ***Find unknown unwanted programs and trojans (Trova minacce di programmi sconosciuti e trojan)***.
    - ***Find unknown macro threats (Trova minacce di macro sconosciute)***.

22. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.

23. Fare clic sulla scheda ***Exclusions (Esclusioni)***, quindi fare clic su ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Set Exclusions (Imposta esclusioni)***.

24. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add Exclusion Item (Aggiungi elemento esclusione)***.

25. Selezionare ***By name/location (Per nome/posizione)*** e fare clic su ***Browse (Sfoglia)***. Viene visualizzata la schermata ***Browse for Files or Folders (Sfoglia file o cartelle)***.

26. Accedere alle ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:***, una alla volta, e selezionare ***OK***.

27. Selezionare ***Also exclude subfolders (Escludi anche sottocartelle)*** nella finestra ***Add Exclusion Item (Aggiungi elemento esclusione)*** e fare clic su ***OK***.

28. Accertarsi che siano presenti le cartelle C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies\, E:\, G:\ nella finestra Set Exclusions (Imposta esclusioni).

29. Fare clic su ***OK***.

30. Fare clic con il pulsante destro del mouse su ***AutoUpdate (Aggiornamento automatico)*** e selezionare ***Properties (Proprietà)***. Viene visualizzata la schermata McAfee AutoUpdate Properties – AutoUpdate (Proprietà aggiornamento automatico McAfee – Aggiornamento automatico).

31. Deselezionare le seguenti opzioni in ***Update Options (Opzioni aggiornamento)***:

    - ***Get new detection engine and dats if available (Ottieni nuovo motore di rilevamento e dat, se disponibili)***.
    - ***Get other available updates (service packs, upgrades, etc.) (Ottieni altri aggiornamenti disponibili (service pack, aggiornamenti ecc.))***.

32. Fare clic su ***Schedule (Programmazione)***. Viene visualizzata la schermata Schedule Settings (Impostazioni programmazione).

33. Deselezionare ***Enable (scheduled task runs at specified time) (Attiva (le operazioni programmate vengono eseguite all'ora specificata))*** in ***Schedule Settings (Impostazioni programmazione)***.

34. Fare clic su ***OK***.

35. Fare clic su ***OK***.

36. Fare clic con il pulsante destro del mouse sulla finestra ***VirusScan Console*** e selezionare ***New On-Demand Scan Task (Nuova attività di scansione su richiesta)***.

37. Rinominare la nuova scansione ***Weekly Scheduled Scan (Scansione programmata settimanale)*.** Viene visualizzata la schermata ***On-Demand Scan Properties - Weekly Scheduled Scan (Proprietà scansione su richiesta - Scansione programmata settimanale)***.

38. Fare clic sulla scheda ***Scan Items (Elementi sottoposti a scansione)*** e deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Options (Opzioni)***.

39. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:

    - ***Find unknown programs threats (Trova minacce programmi indesiderati)*.**
    - ***Find unknown macro threats (Trova minacce di macro sconosciute)*.**

40. Fare clic sulla scheda ***Exclusions (Esclusioni)***, quindi fare clic su ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Set Exclusions (Imposta esclusioni)***.

41. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add Exclusion Item (Aggiungi elemento esclusione)***.

42. Selezionare ***By name/location (Per nome/posizione)*** e fare clic su ***Browse (Sfoglia)***. Viene visualizzata la schermata ***Browse for Files or Folders (Sfoglia file o cartelle)***.

43. Accedere alle cartelle ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:***, una alla volta, e selezionare ***OK***.

44. Selezionare ***Also exclude subfolders (Escludi anche sottocartelle)*** nella finestra ***Add Exclusion Item (Aggiungi elemento esclusione)*** e fare clic su ***OK***.

45. Accertarsi che le cartelle ***C:\Program Files\GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:***, ***G:*** siano presenti nella finestra ***Set Exclusions (Imposta esclusioni)***.

46. Fare clic su ***OK***.

47. Fare clic sulla scheda ***Performance (Prestazioni)*** e selezionare ***Disabled (Disattivato)*** per ***Sensitivity level (Livello sensibilità)*** in ***Artemis (Heuristic network check for suspicious files) (Artemis (Controllo euristico rete per file sospetti))***.

48. Fare clic su ***Schedule (Programmazione)***. Viene visualizzata la schermata ***Schedule Settings (Impostazioni programmazione)***.

49. Fare clic sulla scheda ***Task (Attività)*** e selezionare ***Enable (scheduled task runs at specified time) (Attiva (le operazioni programmate vengono eseguite all'ora specificata))*** in ***Schedule Settings (Impostazioni programmazione)***.

50. Fare clic sulla scheda ***Schedule (Programmazione)*** e selezionare le seguenti opzioni:
    a. Run task (Esecuzione attività): Weekly (Settimanale).
    b. Start Time (Ora di inizio): 12:00 AM
    c. Every (Ogni): 1 Weeks, Sunday (1 settimana, domenica).
51. Fare clic su ***OK***.
52. Fare clic su ***OK***.
53. Fare clic su ***Tools > Alerts (Strumenti > Avvisi)*** nella finestra ***VirusScan Console.*** Viene visualizzata la schermata Alert Properties (Proprietà avvisi).
54. Deselezionare le caselle di spunta ***On-Access Scan (Scansione all'accesso)***, ***On-Demand Scan and scheduled scans (Scansione a richiesta e scansioni programmate)***, ***Email Scan (Scansione email)*** e ***AutoUpdate (Aggiornamento automatico)***.
55. Fare clic su ***Destination (Destinazione)***. Viene visualizzata la schermata ***Alert Manager Client Configuration (Configurazione client Alert Manager)***.
56. Selezionare la casella di spunta ***Disable alerting (Disattiva avvisi)***.
57. Fare clic su ***OK.*** Viene visualizzata la schermata ***Alert Properties (Proprietà avvisi)***.
58. Selezionare la scheda ***Additional Alerting Options (Opzioni aggiuntive avvisi)***.
59. Selezionare l'opzione ***Suppress all alerts (severities 0 to 4) (Disattiva tutti gli avvisi (gravità da 0 a 4))*** dall'elenco a discesa ***Severity Filter (Filtro gravità)***.
60. Selezionare la scheda ***Alert Manager Alerts (Avvisi Alert Manager)***.
61. Deselezionare la casella di spunta ***Access Protection (Protezione accesso)***.
62. Fare clic su ***OK*** per chiudere la finestra ***Alert Properties (Proprietà avvisi)***.
63. Chiudere la finestra ***VirusScan Console***.

McAfee ePolicy Orchestrator

Panoramica dell'installazione

Installare McAfee ePolicy Orchestrator solo in un ambiente Mac-Lab/CardioLab in rete. McAfee ePolicy Orchestrator devono essere installati in un server della console di gestione antivirus server e McAfee VirusScan Enterprise deve essere distribuito nel server Centricity Cardiology INW e nelle workstation di acquisizione/revisione come client. Attenersi alle seguenti istruzioni per installare e configurare McAfee ePolicy Orchestrator.

Le seguenti istruzioni per il push e la configurazione di McAfee VirusScan Enterprise supportano Patch 3, Patch 4, Patch 8 e Patch 9.

La responsabilità degli aggiornamenti antivirus spetta all'ospedale. Aggiornare regolarmente le definizioni, per assicurare che il sistema sia sempre protetto dai virus più recenti.

Linee guida da seguire prima dell'installazione

1. Per il corretto funzionamento, la console di gestione antivirus McAfee deve essere installata attenendosi alle istruzioni fornite da McAfee.
2. Accedere come **Administrator (Amministratore)** o come membro di tale gruppo in tutti i sistemi client (acquisizione, revisione e server INW) per installare il software antivirus.
3. Disattivare Loopback Connection (Connessione loopback). Per ulteriori informazioni, consultare Disattivazione di Loopback Connection (Connessione loopback) a pagina 6.
4. Per l'implementazione di McAfee VirusScan Enterprise 8.8 Patch 9, contattare McAfee per installare i certificati di autenticazione radice UTN-USERFirst-Object e VeriSign Universal solo sui server INW. Una volta installati i certificati, riavviare il sistema.

NOTA: Qualora i certificati di autenticazione radice UTN-USERFirst-Object e VeriSign Universal non siano installati, non sarà possibile installare di McAfee VirusScan Enterprise 8.8 Patch 9 sui server INW.

5. Per una nuova installazione, aggiungere la seguente versione dell'agente al repository master di McAfee ePolicy Orchestrator in McAfee ePolicy Orchestrator Console: ***- McAfee Agent v5.0.5.658***
6. Per una nuova installazione, aggiungere il seguente pacchetto al repository master di McAfee ePolicy Orchestrator in 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).

NOTA: VSE880LMLRP3.zip contiene i pacchetti di installazione Patch 2 e Patch 3. Patch 2 è per le piattaforme con sistemi operativi Windows 7 e Windows Server 2008, Patch 3 è per le piattaforme con sistemi operativi Windows 8 e Windows Server 2012. Il programma di installazione di McAfee installa la patch corretta identificando la versione del sistema operativo Windows.

7. Per una nuova installazione, aggiungere le seguenti estensioni alla tabella estensioni di McAfee ePolicy Orchestrator in McAfee ePolicy Orchestrator Console:
   - McAfee VirusScan Enterprise 8.8 Patch 3: VIRUSSCAN8800 v8.8.0.348 e VIRUSSCANREPORTS v1.2.0.228
   - McAfee VirusScan Enterprise 8.8 Patch 4: VIRUSSCAN8800 v8.8.0.368 e VIRUSSCANREPORTS v1.2.0.236
   - McAfee VirusScan Enterprise 8.8 Patch 8: VIRUSSCAN8800 v8.8.0.511 e VIRUSSCANREPORTS v1.2.0.311
   - McAfee VirusScan Enterprise 8.8 Patch 9: VIRUSSCAN8800 v8.8.0.548 e VIRUSSCANREPORTS v1.2.0.346

NOTA: VIRUSSCAN8800(348).zip e VIRUSSCANREPORTS120(228).zip sono inclusi nel pacchetto McAfee VirusScan Enterprise 8.8 Patch 3.

VIRUSSCAN8800(368).zip e VIRUSSCANREPORTS120(236).zip sono inclusi nel pacchetto McAfee VirusScan Enterprise 8.8 Patch 4.

VIRUSSCAN8800(511).zip e VIRUSSCANREPORTS120(311).zip sono inclusi nel pacchetto McAfee VirusScan Enterprise 8.8 Patch 8.

VIRUSSCAN8800(548).zip e VIRUSSCANREPORTS120(346).zip sono inclusi nel pacchetto McAfee VirusScan Enterprise 8.8 Patch 9.

McAfee ePolicy Orchestrator 5.0 o 5.3.2 - Procedura di distribuzione di una nuova installazione (metodo di installazione push preferito)

1. A seconda della versione del software, selezionare ***Start > All programs (Tutti i programmi) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console (Avvia la console di McAfee ePolicy Orchestrator 5.0.0))*** o ***Start > All Programs (Tutti i programmi) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console (Avvia la console di McAfee ePolicy Orchestrator 5.3.2))*** per accedere alla console di ePolicy Orchestrator.

NOTA: Fare clic su ***Continue with this website (Continuare con il sito Web)*** se viene visualizzata la finestra del messaggio ***Security Alert (Avviso di protezione)***.

2. Inserire nome utente e password e fare clic su ***Log On (Accedi)*.**

3. Selezionare ***Menu > Systems (Sistemi) > Systems Tree (Struttura sistemi)***. Si apre la finestra System Tree (Struttura sistemi).

4. Fare clic su ***My Organization (Organizzazione)*** e quando si attiva ***My Organization (Organizzazione)*** fare clic su ***System Tree Actions (Azioni struttura sistemi) > New Systems (Nuovi sistemi)*** dall'angolo inferiore sinistro della schermata.

5. Selezionare ***Push agents and add systems to the current group (My Organization) (Push agenti e aggiungi sistemi al gruppo corrente (Organizzazione))*** e fare clic su ***Browse (Sfoglia)*** in Target systems (Sistemi di destinazione).

6. Inserire nome utente e password dell'**amministratore locale/di dominio** e fare clic su ***OK***.

7. Selezionare il dominio ***INW*** dall'elenco a discesa ***Domain (Dominio)*.**

8. Selezionare le macchine client (acquisizione, revisione e server INW) collegate al dominio e fare clic su ***OK*.**

NOTA: Se il nome del dominio non è incluso nell'elenco a discesa ***Domain (Dominio)***, procedere come segue:

   - Nelle finestre ***Browse for Systems (Sfoglia sistemi)***, fare clic su ***Cancel (Annulla)***.
   - Nella finestra ***New Systems (Nuovi sistemi)*,** inserire i singoli nomi dei sistemi delle macchine client (acquisizione, revisione e server INW) nel campo ***Target systems (Sistemi di destinazione)*** e proseguire con i passaggi successivi.

9. Per ***Agent Version (Versione agente)*** selezionare ***McAfee Agent for Windows 4.8.0 (Current) (McAfee Agent for Windows 4.8.0 (corrente))*** o ***McAfee Agent for Windows 5.0.4 (Current) (McAfee Agent for Windows 5.0.4 (corrente))***. Inserire nome utente e password dell'**amministratore di dominio** e fare clic su ***OK***.

10. Nelle macchine client (acquisizione, revisione e server INW), accertarsi che le directory vengano create correttamente, a seconda della versione della patch:

    - Per le patch 3 e 4, accertarsi che la directory ***C:\Program Files\McAfee\Common Framework*** sia presente e che McAfee Agent sia installato nella stessa directory.

NOTA: Per il server INW, accertarsi che la directory ***C:\Program Files (x86)\McAfee\Common Framework*** sia presente e che McAfee Agent sia installato nella stessa directory.

    - Per la patch 8, accertarsi che la directory ***C:\Program Files\McAfee\Agent*** sia presente e che McAfee Agent sia installato nella stessa directory.

NOTA: Per il server INW, accertarsi che la directory ***C:\Program Files (x86)\McAfee\Common Framework*** sia presente.

11. Riavviare le macchine client (acquisizione, revisione e server INW) e accedere come **amministratore di dominio** o come membro di tale gruppo.

12. A seconda della versione del software, fare clic su ***Start > All Programs (Tutti i programmi) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console (Avvia la console di McAfee ePolicy Orchestrator 5.0.0)*** o ***Start > All Programs (Tutti i programmi) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console (Avvia la console di McAfee ePolicy Orchestrator 5.3.2)***.

13. Inserire nome utente e password e fare clic su ***Log On (Accedi)***.

14. Fare clic su ***Menu > Systems (Sistemi) > Systems Tree (Struttura sistemi)***.

15. Fare clic su ***My Organization (Organizzazione)*** e quando si attiva ***My Organization (Organizzazione)*** fare clic sulla scheda ***Assigned Client Tasks (Attività client assegnate)***.

16. Fare clic sul pulsante ***Actions (Azioni) > New Client Task Assignment (Nuova assegnazione attività client)*** nella parte inferiore della schermata. Viene visualizzata la schermata Client Task Assignment Builder (Creazione assegnazioni attività client).

17. Selezionare le seguenti opzioni:

    a. **Product (Prodotto):** McAfee Agent

    b. **Task Type (Tipo di attività):** Product Deployment (Distribuzione prodotto)

    c. **Task name (Nome attività):** Create New Task (Crea nuova attività)

18. Nella schermata ***Client Task Catalog: New Task- McAfee Agent: Product Deployment (Catalogo attività client: Nuova attività - McAfee Agent: Distribuzione prodotto)***, compilare i seguenti campi:

    a. **Task name (Nome attività):** Inserire il nome dell'attività

    b. **Target platforms (Piattaforme di destinazione):** Windows

    c. **Products and components (Prodotti e componenti):** Versione di VirusScan Enterprise qualificata per v6.9.6

    d. **Options (Opzioni):** Run at every policy enforcement (Windows only) (Esecuzione con ogni applicazione dei criteri) (solo Windows)) se ***Options (Opzioni)*** è disponibile

19. Fare clic su ***Save (Salva)*.**
20. Nella schermata ***1 Select Task (1 Seleziona attività)***, selezionare le seguenti opzioni:
    a. **Product (Prodotto):** McAfee Agent
    b. **Task Type (Tipo di attività):** Product Deployment (Distribuzione prodotto)
    c. **Task name (Nome attività):** Nome dell'attività appena creata
21. Fare clic su ***Next (Avanti)***. Viene visualizzata la schermata 2 Programmazione.
22. Selezionare ***Run immediately (Esegui immediatamente)*** dall'elenco a discesa ***Schedule type (Tipo di programmazione)***.
23. Fare clic su ***Next (Avanti)***. Viene visualizzata la schermata 3 Riepilogo.
24. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***System Tree (Struttura sistemi)***.
25. Selezionare la scheda ***Systems (Sistemi)*** e scegliere tutte le macchine client (acquisizione, revisione e server INW) connesse al dominio.
26. Fare clic su ***Wake up Agents (Agenti wake up)*** nella parte inferiore della finestra.
27. Lasciare le impostazioni predefinite e fare clic su ***OK***.
28. Attendere che venga visualizzata l'icona di McAfee nella barra delle applicazioni, riavviare tutte le macchine client (acquisizione, revisione e server INW) e accedere come **Administrator (Amministratore)** o come membro di tale gruppo su tutte le macchine client.
29. Fare clic sul collegamento ***Log Off (Esci)*** per chiudere la console di McAfee ePolicy Orchestrator.

McAfee ePolicy Orchestrator 5.9.0 - Procedura di distribuzione di una nuova installazione (metodo di installazione push preferito)

1. Fare clic su ***Start (Start) > All Programs (Tutti i programmi) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console (Avvia la console di McAfee ePolicy Orchestrator 5.9.0)*** per accedere alla console ePolicy Orchestrator.

NOTA: Fare clic su ***Continue with this website (Continuare con il sito Web)*** se viene visualizzata la finestra del messaggio ***Security Alert (Avviso di protezione)***.

2. Inserire nome utente e password e fare clic su ***Log On (Accedi)***.
3. Selezionare ***Menu > Systems (Sistemi) > Systems Tree (Struttura sistemi)***. Si apre la finestra ***System Tree (Struttura sistemi)***.
4. Fare clic su ***My Organization (Organizzazione)*** e quando si attiva ***My Organization (Organizzazione)*** fare clic su ***New Systems (Nuovi sistemi)*** nella parte superiore della schermata.
5. Selezionare ***Push agents and add systems to the current group (My Organization) (Push agenti e aggiungi sistemi al gruppo corrente (Organizzazione))*** e fare clic su ***Browse (Sfoglia)*** in Target systems (Sistemi di destinazione).
6. Inserire nome utente e password dell'**amministratore locale/di dominio** e fare clic su ***OK***.

7. Selezionare il dominio ***INW*** dall'elenco a discesa ***Domain (Dominio)***.
8. Selezionare le macchine client (acquisizione, revisione e server INW) collegate al dominio e fare clic su ***OK*.**

NOTA: Se il nome del dominio non è incluso nell'elenco a discesa ***Domain (Dominio)***, procedere come segue:

- Nelle finestre ***Browse for Systems (Sfoglia sistemi)***, fare clic su ***Cancel (Annulla)*.**
- Nella finestra ***New Systems (Nuovi sistemi)***, inserire manualmente i singoli nomi dei sistemi delle macchine client (acquisizione, revisione e server INW) separati da una virgola nel campo ***Target systems (Sistemi di destinazione)*** e proseguire con i passaggi successivi.

9. Selezionare ***Agent Version (Versione agente)*** come ***McAfee Agent for Windows 5.0.5 (current) (McAfee Agent for Windows 5.0.5 (corrente))***. Inserire nome utente e password dell'**amministratore di dominio** e fare clic su ***OK***.
10. Nelle macchine client (acquisizione, revisione e server INW), confermare che le directory ***C:\Program Files\McAfee\Agent*** vengano create correttamente.
11. Riavviare le macchine client (acquisizione, revisione e server INW) e accedere come **amministratore di dominio** o come membro di tale gruppo.
12. Fare clic su ***Start (Start) > All Programs (Tutti i programmi) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console (Avvia la console di McAfee ePolicy Orchestrator 5.9.0)*** per accedere alla console ePolicy Orchestrator.
13. Inserire nome utente e password e fare clic su ***Log On (Accedi)***.
14. Fare clic su ***Menu > Systems (Sistemi) > Systems Tree (Struttura sistemi)*.**
15. Fare clic su ***My Organization (Organizzazione)*** e quando si attiva ***My Organization (Organizzazione)*** fare clic sulla scheda ***Assigned Client Tasks (Attività client assegnate)***.
16. Fare clic sul pulsante ***Actions (Azioni) > New Client Task Assignment (Nuova assegnazione attività client)*** nella parte inferiore della schermata. Viene visualizzata la schermata ***Client Task Assignment Builder (Creazione assegnazioni attività client)*.**
17. Selezionare le seguenti opzioni:
    a. **Product (Prodotto):** McAfee Agent
    b. **Task Type (Tipo di attività):** Product Deployment (Distribuzione prodotto)
18. Fare clic su ***Task Actions > Create New Task (Azioni attività > Crea nuova attività)***. Viene visualizzata la schermata ***Create New Task (Crea nuova attività)***.
19. Nella schermata ***Create New Task (Crea nuova attività)***, completare i campi come segue:
    a. **Task name (Nome attività):** Inserire il nome dell'attività
    b. **Target platforms (Piattaforme di destinazione):** Windows (deselezionare tutte le altre opzioni)
    c. **Products and components (Prodotti e componenti):** VirusScan Enterprise 8.8.0.1804
20. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***Client Task Assignment Builder (Creazione assegnazioni attività client)***.

21. Nella schermata ***Client Task Assignment Builder (Creazione assegnazioni attività client)*****,** selezionare le seguenti opzioni:

    a. **Product (Prodotto):** McAfee Agent

    b. **Task Type (Tipo di attività):** Product Deployment (Distribuzione prodotto)

    c. **Task name (Nome attività):** Nome dell'attività appena creata

    d. **Schedule Type (Tipo di programmazione):** Eseguire immediatamente

22. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***Assigned Client Tasks (Attività client assegnate)***.

23. Selezionare la scheda ***Systems (Sistemi)*** e scegliere tutte le macchine client (acquisizione, revisione e server INW) connesse al dominio.

24. Fare clic su ***Wake up Agents (Agenti wake up)*** nella parte inferiore della finestra.

25. Lasciare le impostazioni predefinite e fare clic su ***OK***.

26. Attendere che venga visualizzata l'icona di McAfee nella barra delle applicazioni, riavviare tutte le macchine client (acquisizione, revisione e server INW) e accedere come **Administrator (Amministratore)** o come membro di tale gruppo su tutte le macchine client.

27. Fare clic sul collegamento ***Log Off (Esci)*** per chiudere la console di McAfee ePolicy Orchestrator.

Configurazione della console del server di McAfee ePolicy Orchestrator 5.0 e 5.3.2

1. A seconda della versione del software, fare clic su ***Start > All Programs (Tutti i programmi) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console (Avvia la console di McAfee ePolicy Orchestrator 5.0.0)*** o ***Start > All Programs (Tutti i programmi) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console (Avvia la console di McAfee ePolicy Orchestrator 5.3.2)***.

2. Inserire nome utente e password e fare clic su ***Log On (Accedi)***.

3. Fare clic su ***Menu > Systems (Sistemi) > Systems Tree (Struttura sistemi)***.

4. Fare clic su ***My Organization (Organizzazione)*** e quando si attiva My Organization (Organizzazione) fare clic sulla scheda ***Assigned Client Tasks (Attività client assegnate)***.

5. Fare clic su ***Actions (Azioni) > New Client Task Assignment (Nuova assegnazione attività client)*** nella parte inferiore della schermata. Viene visualizzata la schermata ***Client Task Assignment Builder (Creazione assegnazioni attività client)***.

6. Selezionare le seguenti opzioni:

    a. ***Product (Prodotto):*** VirusScan Enterprise 8.8.0

    b. ***Task Type (Tipo di attività):*** On Demand Scan (Scansione a richiesta)

    c. ***Task name (Nome attività):*** Create New Task (Crea nuova attività)

7. Nella schermata ***Client Task Catalog: New Task - VirusScan Enterprise 8.8.0: On Demand Scan (Catalogo attività client: Nuova attività - VirusScan Enterprise 8.8.0: Scansione a richiesta)***, compilare i seguenti campi:

    a. ***Task name (Nome attività):*** Weekly Scheduled Scan (Scansione programmata settimanale)

    b. ***Description (Descrizione):*** Weekly Scheduled Scan (Scansione programmata settimanale)

8. Fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

9. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Options (Opzioni)***.

10. Deselezionare le seguenti opzioni in Heuristics (Euristica):

    - ***Find unknown programs threats (Trova minacce programmi indesiderati)***.
    - ***Find unknown macro threats (Trova minacce di macro sconosciute)***.

11. Fare clic sulla scheda ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Exclusions (Esclusioni)***.

12. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.

13. Selezionare ***By pattern (In base al modello)*** e inserire le cartelle **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:**, una alla volta, quindi selezionare Also exclude subfolders (Escludi anche sottocartelle). Fare clic su ***OK***.

14. Fare clic sulla scheda ***Performance (Prestazioni)***. Viene visualizzata la schermata ***Performance (Prestazioni)***.

15. Selezionare ***Disabled (Disattivata)*** da ***Artemis (Heuristic network check for suspicious files) (Artemis (Controllo euristico rete per file sospetti))***.

16. Fare clic su ***Save (Salva)***.

17. Nella schermata ***1 Select Task (1 Seleziona attività)***, selezionare le seguenti opzioni:

    - ***Product (Prodotto):*** VirusScan Enterprise 8.8.0
    - ***Task Type (Tipo di attività):*** On Demand Scan (Scansione a richiesta)
    - ***Task name (Nome attività):*** Weekly Scheduled Scan (Scansione programmata settimanale)

18. Fare clic su ***Next (Avanti)***. Viene visualizzata la schermata ***2 Schedule (2 Programmazione)***.

19. Selezionare ***Weekly (Settimanale)*** dall'elenco a discesa ***Schedule type (Tipo di programmazione)*** e scegliere ***Sunday (Domenica)***.

20. Per ***Start time (Ora di inizio)*** impostare ***12:00 AM*** e selezionare ***Run Once at that time (Esegui una sola volta a tale ora)***.

21. Fare clic su ***Next (Avanti)***. Viene visualizzata la schermata ***3 Summary (3 Riepilogo)***.

22. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***System Tree (Struttura sistemi)***.

23. Selezionare la scheda ***Assigned Policies (Criteri assegnati)***. Viene visualizzata la schermata ***Assigned Policies (Criteri assegnati)***.

24. Dall'elenco a discesa ***Product (Prodotto)***, selezionare ***VirusScan Enterprise 8.8.0***.

25. Fare clic su ***My Default (Impostazioni predefinite)*** per ***On-Access General Policies (Criteri generali all'accesso)***. Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > On-Access General Policies (Criteri generali all'accesso) > My Default (Impostazioni predefinite)***.

26. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)*** e fare clic sulla scheda ***General (Generale).*** Viene visualizzata la schermata ***General (Generale)***.

27. Selezionare ***Disabled (Disattivata)*** da ***Artemis (Heuristic network check for suspicious files) (Artemis (Controllo euristico rete per file sospetti))***.

28. Fare clic sulla scheda ***ScriptScan.*** Viene visualizzata la schermata ***Script Scan (Scansione script)***.

29. Deselezionare ***Enable scanning of scripts (Attiva scansione degli script).***

30. Fare clic sulla scheda ***Blocking (Blocco)***. Viene visualizzata la schermata ***Blocking (Blocco)***.

31. Deselezionare ***Block the connection when a threatened file is detected in a shared folder (Blocca la connessione quando viene rilevato un file minacciato in una cartella condivisa)***.

32. Selezionare la scheda ***Messages (Messaggi).*** Viene visualizzata la schermata ***Messages (Messaggi)***.

33. Deselezionare ***Show the messages dialog box when a threat is detected and display the specified text in the message (Mostra la finestra di dialogo dei messaggi quando viene rilevata una minaccia e il testo specificato nel messaggio)***.

34. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)*** e fare clic sulla scheda ***General (Generale).*** Viene visualizzata la schermata ***General (Generale)***.

35. Selezionare ***Disabled (Disattivata)*** da ***Artemis (Heuristic network check for suspicious files) (Artemis (Controllo euristico rete per file sospetti))***.

36. Fare clic sulla scheda ***ScriptScan.*** Viene visualizzata la schermata ***Script Scan (Scansione script)***.

37. Accertarsi che l'opzione ***Enable scanning of scripts (Attiva scansione degli script)*** sia deselezionata.

38. Fare clic sulla scheda ***Blocking (Blocco).*** Viene visualizzata la schermata ***Blocking (Blocco)***.

39. Deselezionare ***Block the connection when a threatened file is detected in a shared folder (Blocca la connessione quando viene rilevato un file minacciato in una cartella condivisa)***.

40. Selezionare la scheda ***Messages (Messaggi).*** Viene visualizzata la schermata ***Messages (Messaggi)***.

41. Deselezionare ***Show the messages dialog box when a threat is detected and display the specified text in the message (Mostra la finestra di dialogo dei messaggi quando viene rilevata una minaccia e il testo specificato nel messaggio)***.

42. Fare clic su ***Save (Salva)*.**

43. Fare clic su ***My Default (Impostazioni predefinite)*** per ***On-Access Default Processes Policies (Criteri processi predefiniti all'accesso)***. Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies (Criteri generali all'accesso) > My Default (Impostazioni predefinite)***.

44. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)***.

45. Fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

46. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:

    - ***Find unknown unwanted programs and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***

47. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.

48. Fare clic sulla scheda ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Exclusions (Esclusioni)***.

49. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.

50. Selezionare ***By pattern (In base al modello)*** e inserire le cartelle **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:**, una alla volta, quindi selezionare ***Also exclude subfolders (Escludi anche sottocartelle)***. Fare clic su ***OK***.

51. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)*** e fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

52. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)*:**

    - ***Find unknown unwanted programs and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***

53. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.

54. Fare clic sulla scheda ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Exclusions (Esclusioni)***.

55. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.

56. Selezionare ***By pattern (In base al modello)*** e inserire le cartelle **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies**, una alla volta, quindi selezionare ***Also exclude subfolders (Escludi anche sottocartelle)***. Fare clic su ***OK***.

57. Fare clic su ***Save (Salva)***.

58. Fare clic su ***My Default (Impostazioni predefinite)*** per ***On-Access Low-Risk Processes Policies (Criteri processi a basso rischio all'accesso)***. Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies (Criteri processi a basso rischio all'accesso > My Default (Impostazioni predefinite).***

59. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per).***

60. Fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

61. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:

    - ***Find unknown unwanted programs and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***

62. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.

63. Fare clic sulla scheda ***Exclusions (Esclusioni).*** Viene visualizzata la schermata ***Exclusions (Esclusioni)***.

64. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.

65. Selezionare ***By pattern (In base al modello)*** e inserire le cartelle **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:**, una alla volta, quindi selezionare ***Also exclude subfolders (Escludi anche sottocartelle)***. Fare clic su ***OK***.

66. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)*** e fare clic sulla scheda ***Scan Items (Scansione elementi).*** Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

67. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:

    - ***Find unknown unwanted programs and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***

68. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.

69. Fare clic sulla scheda ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Exclusions (Esclusioni)***.

70. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.

71. Selezionare ***By pattern (In base al modello)*** e inserire le cartelle **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies**, una alla volta, quindi selezionare ***Also exclude subfolders (Escludi anche sottocartelle).*** Fare clic su ***OK***.

72. Fare clic su ***Save (Salva)***.

73. Fare clic su ***My Default (Impostazioni predefinite)*** per ***On-Access High-Risk Processes Policies (Criteri processi ad alto rischio all'accesso).*** Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies (Criteri processi ad alto rischio all'accesso > My Default (Impostazioni predefinite)***.

74. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)*.**

75. Fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

76. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:

    - ***Find unknown unwanted programs and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***

77. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.

78. Fare clic sulla scheda ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Exclusions (Esclusioni)***.

79. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.

80. Selezionare ***By pattern (In base al modello)*** e inserire le cartelle **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:**, una alla volta, quindi selezionare ***Also exclude subfolders (Escludi anche sottocartelle)*.** Fare clic su ***OK***.

81. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)*** e fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

82. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:

    - ***Find unknown unwanted programs and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***

83. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.

84. Fare clic sulla scheda ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Exclusions (Esclusioni)***.

85. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.

86. Selezionare By pattern (In base al modello) e inserire le cartelle **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies**, una alla volta, quindi selezionare ***Also exclude subfolders (Escludi anche sottocartelle)***. Fare clic su ***OK***.

87. Fare clic su ***Save (Salva)***.

88. Fare clic su ***My Default (Impostazioni predefinite)*** per ***On Delivery Email Scan Policies (Criteri scansione email alla consegna)***. Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies (Politiche scansione email all'a consegna) > My Default (Impostazioni predefinite)***.

89. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)***.

90. Fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

91. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)*.**
    - ***Find unknown program threats and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***
    - ***Find attachments with multiple extensions (Trova allegati con più estensioni).***
92. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.
93. Selezionare ***Disabled (Disattivata)*** da ***Artemis (Heuristic network check for suspicious files) (Artemis (Controllo euristico rete per file sospetti))***.
94. Deselezionare ***Enable on-delivery email scanning (Attiva scansione email alla consegna)*** in ***Scanning of email (Scansione email)***.
95. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)*.**
96. Fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.
97. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:
    - ***Find unknown program threats and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***
    - ***Find attachments with multiple extensions (Trova allegati con più estensioni).***
98. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.
99. Selezionare ***Disabled (Disattivata)*** da ***Artemis (Heuristic network check for suspicious files) (Artemis (Controllo euristico rete per file sospetti))***.
100. Deselezionare ***Enable on-delivery email scanning (Attiva scansione email alla consegna)*** in ***Scanning of email (Scansione email)***.
101. Fare clic su ***Save (Salva)***.
102. Fare clic su ***My Default (Impostazioni predefinite)*** per ***General Options Policies (Criteri opzioni generali)***. Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > General Options Policies (Criteri opzioni generali) > My Default (Impostazioni predefinite)***.
103. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)***.
104. Fare clic sulla scheda ***Display Options (Opzioni di visualizzazione)***. Viene visualizzata la schermata ***Display Options (Opzioni di visualizzazione)***.
105. Selezionare le seguenti opzioni in ***Console options (Opzioni console)***:
    - ***Display managed tasks in the client console (Visualizza attività gestite nella console client).***
    - ***Disable default AutoUpdate task schedule (Disattiva programmazione attività aggiornamento automatico predefinita).***
106. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)*.**
107. Fare clic sulla scheda ***Display Options (Opzioni di visualizzazione)*.** Viene visualizzata la schermata ***Display Options (Opzioni di visualizzazione)***.

108. Selezionare le seguenti opzioni in ***Console options (Opzioni console)***.
    - ***Display managed tasks in the client console (Visualizza attività gestite nella console client).***
    - ***Disable default AutoUpdate task schedule (Disattiva programmazione attività aggiornamento automatico predefinita).***
109. Fare clic su ***Save (Salva)***.
110. Fare clic su ***My Default (Impostazioni predefinite)*** per ***Alert Policies (Criteri per gli avvisi)***. Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > Alter Policies (Criteri per gli avvisi) > My Default (Impostazioni predefinite)***.
111. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)***.
112. Fare clic sulla scheda ***Alert Manager Alerts (Avvisi Alert Manager)***. Viene visualizzata la schermata ***Alert Manager Alerts (Avvisi Alert Manager)***.
113. Deselezionare ***On-Access Scan (Scansione all'accesso)***, ***On-Demand Scan and scheduled scans (Scansione a richiesta e scansioni programmate)***, ***Email Scan (Scansione email)*** e ***AutoUpdate (Aggiornamento automatico)*** in ***Components that generate alerts (Componenti che generano avvisi)***.
114. Selezionare ***Disable alerting (Disattiva avvisi)*** nelle opzioni di ***Alert Manager***.
115. Deselezionare ***Access Protection (Protezione accesso)*** in ***Components that generate alerts (Componenti che generano avvisi)***.
116. Fare clic su ***Additional Alerting Options (Opzioni aggiuntive avvisi)***. Viene visualizzata la schermata ***Additional Alerting Options (Opzioni aggiuntive avvisi)***.
117. Nel menu a discesa ***Severity Filters (Filtro gravità)*** selezionare ***Suppress all alerts (severities 0 to 4) (Disattiva tutti gli avvisi (gravità da 0 a 4))***.
118. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)*** e scegliere la scheda ***Alert Manager Alerts (Avvisi Alert Manager)***. Viene visualizzata la schermata ***Alert Manager Alerts (Avvisi Alert Manager)***.
119. Deselezionare ***On-Access Scan (Scansione all'accesso)***, ***On-Demand Scan and scheduled scans (Scansione a richiesta e scansioni programmate)***, ***Email Scan (Scansione email)*** e ***AutoUpdate (Aggiornamento automatico)*** in ***Components that generate alerts (Componenti che generano avvisi)***.
120. Selezionare ***Disable alerting (Disattiva avvisi)*** nelle opzioni di ***Alert Manager***.
121. Deselezionare ***Access Protection (Protezione accesso)*** in ***Components that generate alerts (Componenti che generano avvisi)***.
122. Fare clic su ***Additional Alerting Options (Opzioni aggiuntive avvisi)***. Viene visualizzata la schermata Additional Alerting Options (Opzioni aggiuntive avvisi).
123. Nel menu a discesa ***Severity Filters (Filtro gravità)*** selezionare ***Suppress all alerts (severities 0 to 4) (Disattiva tutti gli avvisi (gravità da 0 a 4))***.
124. Fare clic su ***Save (Salva)***.
125. Fare clic su ***My Default (Impostazioni predefinite)*** per ***Access Protection Policies (Criteri di protezione accesso)***. Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > Access Protection Policies (Criteri di protezione accesso) > My Default (Impostazioni predefinite)***.

126. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)*.**

127. Fare clic sulla scheda ***Access Protection (Protezione accesso)***. Viene visualizzata la schermata ***Access Protection (Protezione accesso)*.**

128. Deselezionare le seguenti opzioni in ***Access protection settings (Impostazioni di protezione accesso)*:**

    - ***Enable access protection (Attiva protezione accesso).***
    - ***Prevent McAfee services from being stopped (Impedisce l'arresto dei servizi McAfee).***

129. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)*.**

130. Fare clic sulla scheda ***Access Protection (Protezione accesso)*.** Viene visualizzata la schermata ***Access Protection (Protezione accesso)*.**

131. Deselezionare le seguenti opzioni in ***Access protection settings (Impostazioni di protezione accesso)*:**

    - ***Enable access protection (Attiva protezione accesso).***
    - ***Prevent McAfee services from being stopped (Impedisce l'arresto dei servizi McAfee).***

132. Fare clic su ***Save (Salva)***.

133. Fare clic su ***My Default (Impostazioni predefinite)*** per ***Buffer Overflow Protection Policies (Criteri di protezione dall'overflow del buffer)*.** Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies (Criteri di protezione dall'overflow del buffer) > My Default (Impostazioni predefinite)***.

134. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)*.**

135. Fare clic sulla scheda ***Buffer Overflow Protection (Criteri di protezione da overflow del buffer)***. Viene visualizzata la schermata ***Buffer Overflow Protection (Protezione da overflow del buffer)***.

136. Deselezionare ***Show the message dialog box when a buffer overflow is detected (Mostra la finestra di dialogo dei messaggi quando viene rilevato un overflow del buffer)*** in ***Client system warning (Avvertenza sistema client)***.

137. Deselezionare ***Enable buffer overflow protection (Attiva protezione da overflow del buffer)*** in ***Buffer overflow settings (Impostazioni overflow del buffer)***.

138. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)***.

139. Fare clic sulla scheda ***Buffer Overflow Protection (Criteri di protezione da overflow del buffer)***. Viene visualizzata la schermata ***Buffer Overflow Protection (Protezione da overflow del buffer)***.

140. Deselezionare ***Show the message dialog box when a buffer overflow is detected (Mostra la finestra di dialogo dei messaggi quando viene rilevato un overflow del buffer)*** in ***Client system warning (Avvertenza sistema client)***.

141. Deselezionare ***Enable buffer overflow protection (Attiva protezione da overflow del buffer)*** in ***Buffer overflow settings (Impostazioni overflow del buffer)***.

142. Fare clic su ***Save (Salva)***.

143. Dal menu a discesa ***Product (Prodotto)***, selezionare ***McAfee Agent***. Viene visualizzata la finestra ***Policies (Criteri)*** per McAfee Agent.

144. Fare clic su ***My Default (Impostazioni predefinite)*** per ***Repository (Archivio)***. Viene visualizzata la schermata ***McAfee Agent > Repository (Archivio) > My Default (Impostazioni predefinite)***.

145. Fare clic sulla scheda ***Proxy***. Viene visualizzata la schermata ***Proxy*.**

146. Selezionare ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX) (Usa impostazioni di Internet Explorer (per Windows)/ Impostazioni preferenze di sistema (per Mac OSX))*** in ***Proxy settings (Impostazioni proxy)***.

147. Fare clic su ***Save (Salva)***.

148. Fare clic sulla scheda ***Systems (Sistemi)***.

149. Selezionare tutti i sistemi client (Acquisizione, Revisione e Server Centricity Cardiology INW) a cui devono essere distribuiti i criteri configurati.

150. Selezionare ***Wake Up Agents (Agenti wake up)***. Viene visualizzata la schermata ***Wake Up Agent (Agente wake up)***.

151. Fare clic su ***OK***.

152. Uscire da ePolicy Orchestrator.

Configurazione della console del server per McAfee ePolicy Orchestrator 5.9.0

1. Accedere alla console di ePolicy Orchestrator: selezionare ***Start (Start) > All Programs (Tutti i programmi) > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console (Avvia la console di McAfee ePolicy Orchestrator 5.9.0)***.

2. Inserire nome utente e password e fare clic su ***Log On (Accedi)***.

3. Fare clic su ***Menu > Systems (Sistemi) > Systems Tree (Struttura sistemi)***.

4. Fare clic su ***My Organization (Organizzazione)*** e quando si attiva My Organization (Organizzazione) fare clic sulla scheda ***Assigned Client Tasks (Attività client assegnate)***.

5. Fare clic su ***Actions (Azioni) > New Client Task Assignment (Nuova assegnazione attività client)*** nella parte inferiore della schermata. Viene visualizzata la schermata ***Client Task Assignment Builder (Creazione assegnazioni attività client)***.

6. Selezionare le seguenti opzioni:

    a. ***Product (Prodotto):*** VirusScan Enterprise 8.8.0

    b. ***Task Type (Tipo di attività):*** On Demand Scan (Scansione a richiesta)

7. Fare clic su ***Create New Task (Crea nuova attività)*** in ***Task Actions (Azioni attività)***. Viene visualizzata la schermata ***Create New Task (Crea nuova attività)***.

8. Nella schermata ***Create New Task (Crea nuova attività)***, completare i campi come segue:

    a. ***Task name (Nome attività):*** Weekly Scheduled Scan (Scansione programmata settimanale)

    b. ***Description (Descrizione):*** Weekly Scheduled Scan (Scansione programmata settimanale)

9. Fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

10. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Options (Opzioni)***.

11. Deselezionare le seguenti opzioni in Heuristics (Euristica):

    - ***Find unknown programs threats (Trova minacce programmi indesiderati).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***

12. Fare clic sulla scheda ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Exclusions (Esclusioni)***.

13. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.

14. Selezionare ***By pattern (In base al modello)*** e inserire le cartelle **C:\Program Files\GE Healthcare\MLCL**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:**, **G:**, una alla volta, quindi selezionare Also exclude subfolders (Escludi anche sottocartelle). Fare clic su ***OK***.

15. Fare clic sulla scheda ***Performance (Prestazioni)***. Viene visualizzata la schermata ***Performance (Prestazioni)***.

16. Selezionare ***Disabled (Disattivata)*** da ***Artemis (Heuristic network check for suspicious files) (Artemis (Controllo euristico rete per file sospetti))***.

17. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***Client Task Assignment Builder (Creazione assegnazioni attività client)***.

18. Nella schermata ***Client Task Assignment Builder (Creazione assegnazioni attività client)*****,** selezionare le seguenti opzioni:

    - ***Product (Prodotto):*** VirusScan Enterprise 8.8.0
    - ***Task Type (Tipo di attività):*** On Demand Scan (Scansione a richiesta)
    - ***Task name (Nome attività):*** Weekly Scheduled Scan (Scansione programmata settimanale)

19. Selezionare ***Weekly (Settimanale)*** dall'elenco a discesa ***Schedule type (Tipo di programmazione)*** e scegliere ***Sunday (Domenica)***.

20. Per ***Start time (Ora di inizio)*** impostare ***12:00 AM*** e selezionare ***Run Once at that time (Esegui una sola volta a tale ora)***.

21. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***Assigned Client Tasks (Attività client assegnate)***.

22. Selezionare la scheda ***Assigned Policies (Criteri assegnati)***. Viene visualizzata la schermata ***Assigned Policies (Criteri assegnati)***.

23. Dall'elenco a discesa ***Product (Prodotto)***, selezionare ***VirusScan Enterprise 8.8.0***.

24. Fare clic su ***My Default (Impostazioni predefinite)*** per ***On-Access General Policies (Criteri generali all'accesso)***. Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > On-Access General Policies (Criteri generali all'accesso) > My Default (Impostazioni predefinite)***.

25. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)*** e fare clic sulla scheda ***General (Generale)***. Viene visualizzata la schermata ***General (Generale)***.

26. Selezionare ***Disabled (Disattivata)*** da ***Artemis (Heuristic network check for suspicious files) (Artemis (Controllo euristico rete per file sospetti))***.

27. Fare clic sulla scheda ***ScriptScan***. Viene visualizzata la schermata ***Script Scan (Scansione script)***.

28. Deselezionare ***Enable scanning of scripts (Attiva scansione degli script)***.

29. Fare clic sulla scheda ***Blocking (Blocco)***. Viene visualizzata la schermata ***Blocking (Blocco)***.

30. Deselezionare ***Block the connection when a threatened file is detected in a shared folder (Blocca la connessione quando viene rilevato un file minacciato in una cartella condivisa)***.

31. Selezionare la scheda ***Messages (Messaggi)***. Viene visualizzata la schermata ***Messages (Messaggi)***.

32. Deselezionare ***Show the messages dialog box when a threat is detected and display the specified text in the message (Mostra la finestra di dialogo dei messaggi quando viene rilevata una minaccia e il testo specificato nel messaggio)***.

33. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)*** e fare clic sulla scheda ***General (Generale)***. Viene visualizzata la schermata ***General (Generale)***.

34. Selezionare ***Disabled (Disattivata)*** da ***Artemis (Heuristic network check for suspicious files) (Artemis (Controllo euristico rete per file sospetti))***.

35. Fare clic sulla scheda ***ScriptScan***. Viene visualizzata la schermata ***Script Scan (Scansione script)***.

36. Accertarsi che l'opzione ***Enable scanning of scripts (Attiva scansione degli script)*** sia deselezionata.

37. Fare clic sulla scheda ***Blocking (Blocco)***. Viene visualizzata la schermata ***Blocking (Blocco)***.

38. Deselezionare ***Block the connection when a threatened file is detected in a shared folder (Blocca la connessione quando viene rilevato un file minacciato in una cartella condivisa)***.

39. Selezionare la scheda ***Messages (Messaggi)***. Viene visualizzata la schermata ***Messages (Messaggi)***.

40. Deselezionare ***Show the messages dialog box when a threat is detected and display the specified text in the message (Mostra la finestra di dialogo dei messaggi quando viene rilevata una minaccia e il testo specificato nel messaggio)***.

41. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata Assigned Policies (Criteri assegnati).

42. Fare clic su ***My Default (Impostazioni predefinite)*** per ***On-Access Default Processes Policies (Criteri processi predefiniti all'accesso)***. Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies (Criteri generali all'accesso) > My Default (Impostazioni predefinite)***.

43. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)***.

44. Fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

45. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:

    - ***Find unknown unwanted programs and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***

46. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.

47. Fare clic sulla scheda ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Exclusions (Esclusioni)***.

48. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.

49. Selezionare ***By pattern (In base al modello)*** e inserire le cartelle **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:**, una alla volta, quindi selezionare ***Also exclude subfolders (Escludi anche sottocartelle)***. Fare clic su ***OK***.

50. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)*** e fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

51. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:

    - ***Find unknown unwanted programs and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***

52. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.

53. Fare clic sulla scheda ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Exclusions (Esclusioni)***.

54. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.

55. Selezionare ***By pattern (In base al modello)*** e inserire le cartelle **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies**, una alla volta, quindi selezionare ***Also exclude subfolders (Escludi anche sottocartelle)***. Fare clic su ***OK***.

56. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***Assigned Policies (Criteri assegnati)***.

57. Fare clic su ***My Default (Impostazioni predefinite)*** per ***On-Access Low-Risk Processes Policies (Criteri processi a basso rischio all'accesso)***. Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies (Criteri processi a basso rischio all'accesso > My Default (Impostazioni predefinite)***.

58. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)***.

59. Fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

60. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:

    - ***Find unknown unwanted programs and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***

61. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.

62. Fare clic sulla scheda ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Exclusions (Esclusioni)***.

63. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.

64. Selezionare ***By pattern (In base al modello)*** e inserire le cartelle **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:**, una alla volta, quindi selezionare ***Also exclude subfolders (Escludi anche sottocartelle)*.** Fare clic su ***OK***.

65. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)*** e fare clic sulla scheda ***Scan Items (Scansione elementi)*.** Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

66. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:

    - ***Find unknown unwanted programs and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***

67. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.

68. Fare clic sulla scheda ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Exclusions (Esclusioni)***.

69. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.

70. Selezionare ***By pattern (In base al modello)*** e inserire le cartelle **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies**, una alla volta, quindi selezionare ***Also exclude subfolders (Escludi anche sottocartelle)***. Fare clic su ***OK***.

71. Fare clic su ***Save (Salva)*.** Viene visualizzata la schermata ***Assigned Policies (Criteri assegnati)***.

72. Fare clic su ***My Default (Impostazioni predefinite)*** per ***On-Access High-Risk Processes Policies (Criteri processi ad alto rischio all'accesso)*.** Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies (Criteri processi ad alto rischio all'accesso > My Default (Impostazioni predefinite)***.

73. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)***.

74. Fare clic sulla scheda ***Scan Items (Scansione elementi)*.** Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

75. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:
    - ***Find unknown unwanted programs and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***
76. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.
77. Fare clic sulla scheda ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Exclusions (Esclusioni)***.
78. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.
79. Selezionare ***By pattern (In base al modello)*** e inserire le cartelle **C:\Program Files\GE Healthcare\MLCL**, **D:\GEData\Studies**, **E:**, **G:**, una alla volta, quindi selezionare ***Also exclude subfolders (Escludi anche sottocartelle)***. Fare clic su ***OK***.
80. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)*** e fare clic sulla scheda ***Scan Items (Scansione elementi).*** Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.
81. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:
    - ***Find unknown unwanted programs and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***
82. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.
83. Fare clic sulla scheda ***Exclusions (Esclusioni)***. Viene visualizzata la schermata ***Exclusions (Esclusioni)***.
84. Fare clic su ***Add (Aggiungi)***. Viene visualizzata la schermata ***Add/Edit Exclusion Item (Aggiungi/modifica elemento esclusione)***.
85. Selezionare By pattern (In base al modello) e inserire le cartelle **C:\Program Files (x86)\GE Healthcare\MLCL**, **D:\GEData\Studies**, una alla volta, quindi selezionare ***Also exclude subfolders (Escludi anche sottocartelle)***. Fare clic su ***OK***.
86. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***Assigned Policies (Criteri assegnati)***.
87. Fare clic su ***My Default (Impostazioni predefinite)*** per ***On Delivery Email Scan Policies (Criteri scansione email alla consegna)***. Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies (Politiche scansione email all'a consegna) > My Default (Impostazioni predefinite)***.
88. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)***.
89. Fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.

90. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***.
    - ***Find unknown program threats and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***
    - ***Find attachments with multiple extensions (Trova allegati con più estensioni).***
91. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.
92. Selezionare ***Disabled (Disattivata)*** da ***Artemis (Heuristic network check for suspicious files) (Artemis (Controllo euristico rete per file sospetti))***.
93. Deselezionare ***Enable on-delivery email scanning (Attiva scansione email alla consegna)*** in ***Scanning of email (Scansione email)***.
94. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)***.
95. Fare clic sulla scheda ***Scan Items (Scansione elementi)***. Viene visualizzata la schermata ***Scan Items (Scansione elementi)***.
96. Deselezionare le seguenti opzioni in ***Heuristics (Euristica)***:
    - ***Find unknown program threats and trojans (Trova minacce di programmi sconosciuti e trojan).***
    - ***Find unknown macro threats (Trova minacce di macro sconosciute).***
    - ***Find attachments with multiple extensions (Trova allegati con più estensioni).***
97. Deselezionare ***Detect unwanted programs (Rileva programmi indesiderati)*** in ***Unwanted programs detection (Rilevamento programmi indesiderati)***.
98. Selezionare ***Disabled (Disattivata)*** da ***Artemis (Heuristic network check for suspicious files) (Artemis (Controllo euristico rete per file sospetti))***.
99. Deselezionare ***Enable on-delivery email scanning (Attiva scansione email alla consegna)*** in ***Scanning of email (Scansione email)***.
100. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***Assigned Policies (Criteri assegnati)***.
101. Fare clic su ***My Default (Impostazioni predefinite)*** per ***General Options Policies (Criteri opzioni generali)***. Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > General Options Policies (Criteri opzioni generali) > My Default (Impostazioni predefinite)***.
102. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)***.
103. Fare clic sulla scheda ***Display Options (Opzioni di visualizzazione)***. Viene visualizzata la schermata ***Display Options (Opzioni di visualizzazione)***.
104. Selezionare le seguenti opzioni in ***Console options (Opzioni console)*:**
    - ***Display managed tasks in the client console (Visualizza attività gestite nella console client).***
    - ***Disable default AutoUpdate task schedule (Disattiva programmazione attività aggiornamento automatico predefinita).***
105. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)***.
106. Fare clic sulla scheda ***Display Options (Opzioni di visualizzazione)***. Viene visualizzata la schermata ***Display Options (Opzioni di visualizzazione)***.

107. Selezionare le seguenti opzioni in ***Console options (Opzioni console)***.
    - ***Display managed tasks in the client console (Visualizza attività gestite nella console client).***
    - ***Disable default AutoUpdate task schedule (Disattiva programmazione attività aggiornamento automatico predefinita).***
108. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***Assigned Policies (Criteri assegnati)***.
109. Fare clic su ***My Default (Impostazioni predefinite)*** per ***Alert Policies (Criteri per gli avvisi)***. Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > Alter Policies (Criteri per gli avvisi) > My Default (Impostazioni predefinite)***.
110. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)***.
111. Fare clic sulla scheda ***Alert Manager Alerts (Avvisi Alert Manager)***. Viene visualizzata la schermata ***Alert Manager Alerts (Avvisi Alert Manager)***.
112. Deselezionare ***On-Access Scan (Scansione all'accesso)***, ***On-Demand Scan and scheduled scans (Scansione a richiesta e scansioni programmate)***, ***Email Scan (Scansione email)*** e ***AutoUpdate (Aggiornamento automatico)*** in ***Components that generate alerts (Componenti che generano avvisi)***.
113. Selezionare ***Disable alerting (Disattiva avvisi)*** nelle opzioni di ***Alert Manager***.
114. Deselezionare ***Access Protection (Protezione accesso)*** in ***Components that generate alerts (Componenti che generano avvisi)***.
115. Fare clic su ***Additional Alerting Options (Opzioni aggiuntive avvisi).*** Viene visualizzata la schermata ***Additional Alerting Options (Opzioni aggiuntive avvisi)***.
116. Nel menu a discesa ***Severity Filters (Filtro gravità)*** selezionare ***Suppress all alerts (severities 0 to 4) (Disattiva tutti gli avvisi (gravità da 0 a 4))***.
117. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)*** e scegliere la scheda ***Alert Manager Alerts (Avvisi Alert Manager)***. Viene visualizzata la schermata ***Alert Manager Alerts (Avvisi Alert Manager)***.
118. Deselezionare ***On-Access Scan (Scansione all'accesso)***, ***On-Demand Scan and scheduled scans (Scansione a richiesta e scansioni programmate)***, ***Email Scan (Scansione email)*** e ***AutoUpdate (Aggiornamento automatico)*** in ***Components that generate alerts (Componenti che generano avvisi)***.
119. Selezionare ***Disable alerting (Disattiva avvisi)*** nelle opzioni di ***Alert Manager***.
120. Deselezionare ***Access Protection (Protezione accesso)*** in ***Components that generate alerts (Componenti che generano avvisi)***.
121. Fare clic su ***Additional Alerting Options (Opzioni aggiuntive avvisi).*** Viene visualizzata la schermata Additional Alerting Options (Opzioni aggiuntive avvisi).
122. Nel menu a discesa ***Severity Filters (Filtro gravità)*** selezionare ***Suppress all alerts (severities 0 to 4) (Disattiva tutti gli avvisi (gravità da 0 a 4))***.
123. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***Assigned Policies (Criteri assegnati)***.

124. Fare clic su ***My Default (Impostazioni predefinite)*** per ***Access Protection Policies (Criteri di protezione accesso)*****.** Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > Access Protection Policies (Criteri di protezione accesso) > My Default (Impostazioni predefinite)***.

125. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)***.

126. Fare clic sulla scheda ***Access Protection (Protezione accesso)***. Viene visualizzata la schermata ***Access Protection (Protezione accesso)***.

127. Deselezionare le seguenti opzioni in ***Access protection settings (Impostazioni di protezione accesso)***:

    - ***Enable access protection (Attiva protezione accesso).***
    - ***Prevent McAfee services from being stopped (Impedisce l'arresto dei servizi McAfee).***
    - ***Enable Enhanced Self-Protection (Attiva protezione automatica avanzata).***

128. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)***.

129. Fare clic sulla scheda ***Access Protection (Protezione accesso)***. Viene visualizzata la schermata ***Access Protection (Protezione accesso)***.

130. Deselezionare le seguenti opzioni in ***Access protection settings (Impostazioni di protezione accesso)***:

    - ***Enable access protection (Attiva protezione accesso).***
    - ***Prevent McAfee services from being stopped (Impedisce l'arresto dei servizi McAfee).***
    - ***Enable Enhanced Self-Protection (Attiva protezione automatica avanzata).***

131. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***Assigned Policies (Criteri assegnati)***.

132. Fare clic su ***My Default (Impostazioni predefinite)*** per ***Buffer Overflow Protection Policies (Criteri di protezione dall'overflow del buffer)*****.** Viene visualizzata la schermata ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies (Criteri di protezione dall'overflow del buffer) > My Default (Impostazioni predefinite)***.

133. Selezionare ***Workstation*** dall'elenco a discesa ***Settings for (Impostazioni per)***.

134. Fare clic sulla scheda ***Buffer Overflow Protection (Criteri di protezione da overflow del buffer)***. Viene visualizzata la schermata ***Buffer Overflow Protection (Protezione da overflow del buffer)***.

135. Deselezionare ***Show the message dialog box when a buffer overflow is detected (Mostra la finestra di dialogo dei messaggi quando viene rilevato un overflow del buffer)*** in ***Client system warning (Avvertenza sistema client)***.

136. Deselezionare ***Enable buffer overflow protection (Attiva protezione da overflow del buffer)*** in ***Buffer overflow settings (Impostazioni overflow del buffer)***.

137. Selezionare ***Server*** dall'elenco a discesa ***Settings for (Impostazioni per)***.

138. Fare clic sulla scheda ***Buffer Overflow Protection (Criteri di protezione da overflow del buffer).*** Viene visualizzata la schermata ***Buffer Overflow Protection (Protezione da overflow del buffer)***.

139. Deselezionare ***Show the message dialog box when a buffer overflow is detected (Mostra la finestra di dialogo dei messaggi quando viene rilevato un overflow del buffer)*** in ***Client system warning (Avvertenza sistema client)***.

140. Deselezionare ***Enable buffer overflow protection (Attiva protezione da overflow del buffer)*** in ***Buffer overflow settings (Impostazioni overflow del buffer)***.

141. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***Assigned Policies (Criteri assegnati)***.

142. Dal menu a discesa ***Product (Prodotto)***, selezionare ***McAfee Agent***. Viene visualizzata la finestra ***Policies (Criteri)*** per McAfee Agent.

143. Fare clic su ***My Default (Impostazioni predefinite)*** per ***Repository (Archivio)***. Viene visualizzata la schermata ***McAfee Agent > Repository (Archivio) > My Default (Impostazioni predefinite)***.

144. Fare clic sulla scheda ***Proxy***. Viene visualizzata la schermata ***Proxy***.

145. Accertarsi che ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX) (Usa impostazioni di Internet Explorer (per Windows)/ Impostazioni preferenze di sistema (per Mac OSX))*** in ***Proxy settings (Impostazioni proxy)*** sia selezionato.

146. Fare clic su ***Save (Salva)***. Viene visualizzata la schermata ***Assigned Policies (Criteri assegnati)***.

147. Fare clic sulla scheda ***Systems (Sistemi)***.

148. Selezionare tutti i sistemi client (acquisizione, revisione e server Centricity Cardiology INW) a cui devono essere distribuiti i criteri configurati.

149. Selezionare ***Wake Up Agents (Agenti wake up)***. Viene visualizzata la schermata ***Wake Up Agent (Agente wake up)***.

150. Fare clic su ***OK***.

151. Uscire da ePolicy Orchestrator.

Linee guida da seguire dopo l'installazione di McAfee ePolicy Orchestrator

Attivare Loopback Connection (Connessione loopback). Per ulteriori informazioni, consultare Attivazione di Loopback Connection (Connessione loopback) a pagina 6.

Trend Micro OfficeScan Client/Server Edition 10.6 SP2

Panoramica dell'installazione

Installare Trend Micro OfficeScan Client/Server Edition solo in un ambiente di rete Mac-Lab/CardioLab. Trend Micro OfficeScan deve essere installato sul server della console di gestione antivirus e distribuito nel server Centricity Cardiology INW e nelle workstation di acquisizione/revisione come client. Attenersi alle seguenti istruzioni per installare ***Trend Micro OfficeScan Client/Server Edition***.

La responsabilità degli aggiornamenti antivirus spetta all'ospedale. Aggiornare regolarmente le definizioni, per assicurare che il sistema sia sempre protetto dai virus più recenti.

Linee guida da seguire prima dell'installazione

1. Si presuppone che la console di gestione antivirus di Trend Micro sia installata in base alle istruzioni di Trend Micro e che funzioni correttamente.
2. Durante l'installazione di Trend Micro OfficeScan, effettuare le seguenti operazioni sul server della console di gestione antivirus:
    a. Deselezionare ***Enable firewall (Attiva firewall)*** nella finestra ***Anti-virus Feature (Funzione antivirus)***.
    b. Selezionare ***No, Please do not enable assessment mode (Non attivare la modalità di valutazione)*** nella finestra ***Anti-spyware Feature (Funzione antispyware)***.
    c. Deselezionare ***Enable web reputation policy (Attiva criterio di reputazione Web)*** nella finestra ***Web Reputation Feature (Funzione reputazione Web)***.
3. Si sconsiglia di utilizzare Trend Micro OfficeScan assieme alla funzione ***CO_2*** con PDM nei sistemi Mac-Lab/CardioLab.
4. Se Trend Micro OfficeScan è necessario:
    a. È preferibile configurare un server della console di gestione antivirus di Trend Micro separato per i sistemi Mac-Lab/CardioLab. È necessaria una modifica globale delle impostazioni antivirus per utilizzare la funzione ***CO_2*** con PDM nei sistemi Mac-Lab/CardioLab.
    b. Se non è possibile configurare un server della console di gestione antivirus di Trend Micro separato, è necessaria una modifica delle impostazioni globali del server della console di gestione antivirus di Trend Micro dopo l'installazione. Questa modifica riguarda tutti i sistemi client connessi al server della console di gestione antivirus di Trend Micro e deve essere esaminata con il personale IT prima di procedere.
5. Accedere come **Administrator (Amministratore)** o come membro di tale gruppo in tutti i sistemi client (acquisizione, revisione e server INW) per installare il software antivirus.
6. Disattivare Loopback Connection (Connessione loopback). Per ulteriori informazioni, consultare Disattivazione di Loopback Connection (Connessione loopback) a pagina 6.
7. Configurare il servizio Browser di computer. Per ulteriori informazioni, consultare Configurazione del servizio Browser di computer prima dell'installazione dell'antivirus a pagina 7.

Trend Micro OfficeScan - Procedura di distribuzione di una nuova installazione (metodo di installazione push preferito)

1. Fare clic su ***Start > All Programs (Tutti i programmi) > Server TrendMicro OfficeScan - <server name> (<nome server>) > Console Web di OfficeScan***.

NOTA: Continuare selezionando ***Continue with this website (Continuare con il sito Web) (Continuare con il sito Web (scelta non consigliata))***. Nella finestra Security Alert (Avviso di protezione), selezionare ***In the future, do not show this warning (Non mostrare l'avviso in futuro)*** e fare clic su ***OK***.

2. Se si ottiene un errore di certificato indicante che il sito non è attendibile, gestire i certificati includendo Trend Micro OfficeScan.
3. Se viene chiesto, installare i componenti aggiuntivi ***AtxEnc***. Viene visualizzata la schermata Security Warning (Avviso di protezione).
4. Fare clic su ***Install (Installa)***.
5. Inserire nome utente e password e fare clic su ***Log On (Accedi)***.
6. Se viene chiesto, fare clic su ***Update Now (Aggiorna ora)*** per installare nuovi widget. Attendere l'aggiornamento dei nuovi. Viene visualizzata la schermata indicante che l'aggiornamento è terminato.
7. Fare clic su ***OK***.
8. Dalla barra dei menu a sinistra, fare clic su ***Networked Computers (Computer in rete) > Client Installation (Installazione client) > Remote (Remota)***.
9. Se viene chiesto, installare i componenti aggiuntivi ***AtxConsole***. Viene visualizzata la schermata Security Warning (Avviso di protezione).
10. Fare clic su ***Install (Installa)***.
11. Fare doppio clic su ***My Company (La mia azienda)*** nella finestra ***Remote Installation (Installazione remota)***. Vengono elencati tutti i domini in ***My Company (La mia azienda)***.
12. Espandere il dominio (ad esempio: INW) dall'elenco. Vengono visualizzati tutti i sistemi connessi al dominio.
13. Se non vengono elencati né domini né sistemi nella finestra ***Domain and Computers (Domini e computer)***, per ogni sistema client (acquisizione, revisione e server INW) effettuare le seguenti operazioni:
    a. Accedere come Administrator (Amministratore) o come membro di tale gruppo su tutte le macchine client.
    b. Fare clic su ***Start > Run (Esegui)***.
    c. Digitare ***\\<Anti-Virus Management Console_server_IP_address> (\\<indirizzo_IP_server_console_gestione_antivirus>)*** e premere ***Invio***. Quando viene chiesto, inserire nome utente e password dell'amministratore.
    d. Accedere a ***\\<Anti-Virus Management Console_server_IP _address>\ofsscan (\\<indirizzo_IP_server_console_gestione_antivirus>\ofsscan)*** e fare doppio clic su ***AutoPcc.exe***. Quando viene chiesto, inserire nome utente e password dell'amministratore.

e. Al termine dell'installazione, riavviare i sistemi client.

f. Accedere come **Administrator (Amministratore)** o come membro di tale gruppo su tutte le macchine client e attendere che l'icona di Trend Micro OfficeScan nella barra delle applicazioni diventi blu.

g. Saltare i rimanenti passaggi di questa procedura e passare alla procedura di configurazione della console del server di Trend Micro OfficeScan.

14. Selezionare le macchine client (acquisizione, revisione e server INW) e fare clic su ***Add (Aggiungi)***.
15. Digitare <nome dominio>\nome utente e password e fare clic su ***Log on (Accedi)***.
16. Selezionare le macchine client (acquisizione, revisione e server INW), una alla volta, dal riquadro ***Selected Computers (Computer selezionati)*** e fare clic su ***Install (Installa)***.
17. Fare clic su ***Yes (Sì)*** nella finestra di conferma.
18. Fare clic su ***OK*** nella finestra del messaggio ***Number of clients to which notifications were sent (Numero di client a cui sono state inviate le notifiche)***.
19. Riavviare tutte le macchine client (acquisizione, revisione e server INW) e accedere come Administrator (Amministratore) o come membro di tale gruppo su tutte le macchine client, quindi attendere che l'icona di Trend Micro OfficeScan nella barra delle applicazioni diventi blu con un segno di spunta verde.
20. Fare clic sul collegamento ***Log Off (Esci)*** per chiudere la ***console Web di OfficeScan***.

Configurazione della console del server di Trend Micro OfficeScan

1. Selezionare ***Start > All Programs (Tutti i programmi) > Server TrendMicro OfficeScan - <server name> (<nome server>) > OfficeScan Web Console (Console Web di OfficeScan)***. Viene visualizzata la schermata ***Trend Micro OfficeScan Login (Accesso a Trend Micro OfficeScan)***.
2. Inserire nome utente e password e fare clic su ***Login (Accedi)***. Viene visualizzata la schermata ***Summary (Riepilogo)***.
3. Dal riquadro a sinistra, selezionare il collegamento ***Networked Computers (Computer in rete) > Client Management (Gestione client)***.
4. Sul lato destro, selezionare ***OfficeScan Server (Server OfficeScan)***.
5. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Scan Settings (Impostazioni scansione) > Manual Scan Settings (Impostazioni per la scansione manuale)***. Viene visualizzata la schermata ***Manual Scan Settings (Impostazioni per la scansione manuale)***.
6. Fare clic sulla scheda ***Target (Destinazione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
   - ***Files to Scan (File da analizzare) > File types scanned by IntelliScan (Tipi di file analizzati da IntelliScan).***
   - ***Scan Settings (Impostazioni scansione) > Scan compressed files (Analizza file compressi).***
   - ***Scan Settings (Impostazioni scansione) > Scan OLE objects (Analizza oggetti OLE).***

- ***Virus/Malware Scan settings only (Solo impostazioni di scansione virus/malware) > Scan boot area (Analizza area di avvio).***
- ***CPU Usage (Utilizzo CPU) > Low (Basso).***
- ***Scan Exclusion (Esclusioni dalla scansione) > Enable scan exclusion (Attiva esclusioni dalla scansione).***
- ***Scan Exclusion (Esclusioni dalla scansione) > Apply scan exclusion settings to all scan types (Applica impostazioni di esclusione dalla scansione a tutti i tipi di scansione).***
- ***Scan Exclusion List (Directories) (Elenco esclusioni dalla scansione (directory)) > Exclude directories where Trend Micro products are installed and select Add path to client Computers Exclusion list (Escludi directory in cui sono installati i prodotti Trend Micro e seleziona percorso di aggiunta all'elenco di esclusione dei computer client).***
- Inserire le cartelle **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL, D:\GEData\Studies**, **E:** e **G:**, una alla volta, e fare clic su ***Add (Aggiungi)***.

7. Fare clic su ***Apply to All Clients (Applica a tutti i client)***.
8. Fare clic su ***OK*** nel messaggio ***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier. Do you want to proceed? (L'elenco esclusioni in questa schermata sostituirà quello nei client o nei domini selezionati precedentemente nella struttura client. Procedere?)***.
9. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Manual Scan Settings (Impostazioni per la scansione manuale)***.
10. Dal riquadro a sinistra, selezionare il collegamento ***Networked Computers (Computer in rete) > Client Management (Gestione client)***.
11. Sul lato destro, selezionare ***OfficeScan Server (Server OfficeScan)***.
12. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Scan Settings (Impostazioni scansione) > Real-time Scan Settings (Impostazioni di scansione in tempo reale)***. Viene visualizzata la schermata ***Real-time Scan Settings (Impostazioni di scansione in tempo reale)***.
13. Fare clic sulla scheda ***Target (Destinazione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
    - ***Real-Time Scan Settings (Impostazioni di scansione in tempo reale) > Enable virus/malware scan (Attiva scansione virus/malware).***
    - ***Real-Time Scan Settings (Impostazioni di scansione in tempo reale) > Enable spyware/grayware scan (Attiva scansione spyware/grayware).***
    - ***Files to Scan (File da analizzare) > File types scanned by IntelliScan (Tipi di file analizzati da IntelliScan).***
    - ***Scan Settings (Impostazioni scansione) > Scan compressed files (Analizza file compressi).***
    - ***Scan Settings (Impostazioni scansione) > Scan OLE objects (Analizza oggetti OLE).***
    - ***Virus/Malware Scan Settings Only (Solo impostazioni di scansione virus/malware) > Enable IntelliTrap (Attiva IntelliTrap).***
    - ***Scan Exclusion (Esclusioni dalla scansione) > Enable scan exclusion (Attiva esclusioni dalla scansione).***

- ***Scan Exclusion (Esclusioni dalla scansione) > Apply scan exclusion settings to all scan types (Applica impostazioni di esclusione dalla scansione a tutti i tipi di scansione).***
- ***Scan Exclusion List (Directories) (Elenco esclusioni dalla scansione (directory)) > Exclude directories where Trend Micro products are installed (Escludi directory in cui sono installati i prodotti Trend Micro).***
- Accertarsi che i percorsi delle cartelle ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** e ***G:*** siano presenti in ***Exclusion List (Elenco esclusioni)***.

14. Fare clic sulla scheda ***Action (Azione)***.
15. Lasciare le impostazioni predefinite e deselezionare le seguenti opzioni:
    - ***Virus/Malware > Display a notification message on the client computer virus/ malware is detected (Visualizza un messaggio di notifica sul computer client al rilevamento di virus/malware).***
    - ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected (Visualizza un messaggio di notifica sul computer client al rilevamento di spyware/grayware).***
16. Fare clic su ***Apply to All Clients (Applica a tutti i client)***.
17. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Real-time Scan Settings (Impostazioni di scansione in tempo reale)***.
18. Dal riquadro a sinistra, selezionare il collegamento ***Networked Computers (Computer in rete) > Client Management (Gestione client)***.
19. Sul lato destro, selezionare ***OfficeScan Server (Server OfficeScan)***.
20. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Scan Settings (Impostazioni scansione) > Scheduled Scan Settings (Impostazioni per la scansione programmata)***. Viene visualizzata la schermata ***Scheduled Scan Settings (Impostazioni per la scansione programmata)***.
21. Fare clic sulla scheda ***Target (Destinazione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
    - ***Scheduled Scan Settings (Impostazioni per la scansione programmata) > Enable virus/malware scan (Attiva scansione virus/malware).***
    - ***Scheduled Scan Settings (Impostazioni per la scansione programmata) > Enable spyware/grayware scan (Attiva scansione spyware/grayware).***
    - ***Schedule (Programmazione) > Weekly, every Sunday, Start time: 00:00 hh:mm (Settimanale, ogni domenica, ora di inizio: 00:00 hh:mm).***
    - ***Files to Scan (File da analizzare) > File types scanned by IntelliScan (Tipi di file analizzati da IntelliScan).***
    - ***Scan Settings (Impostazioni scansione) > Scan compressed files (Analizza file compressi).***
    - ***Scan Settings (Impostazioni scansione) > Scan OLE objects (Analizza oggetti OLE).***
    - ***Virus/Malware Scan settings only (Solo impostazioni di scansione virus/malware) > Scan boot area (Analizza area di avvio).***
    - ***CPU Usage (Utilizzo CPU) > Low (Basso).***
    - ***Scan Exclusion (Esclusioni dalla scansione) > Enable scan exclusion (Attiva esclusioni dalla scansione).***

- ***Scan Exclusion (Esclusioni dalla scansione) > Apply scan exclusion settings to all scan types (Applica impostazioni di esclusione dalla scansione a tutti i tipi di scansione).***
- ***Scan Exclusion List (Directories) (Elenco esclusioni dalla scansione (directory)) > Exclude directories where Trend Micro products are installed (Escludi directory in cui sono installati i prodotti Trend Micro).***
- Accertarsi che i percorsi delle cartelle ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** e ***G:*** siano presenti in Exclusion List (Elenco esclusioni).

22. Fare clic sulla scheda ***Action (Azione)***.
23. Lasciare le impostazioni predefinite e deselezionare le seguenti opzioni:
    - ***Virus/Malware > Display a notification message on the client computer virus/malware is detected (Visualizza un messaggio di notifica sul computer client al rilevamento di virus/malware).***
    - ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected (Visualizza un messaggio di notifica sul computer client al rilevamento di spyware/grayware).***
24. Fare clic su ***Apply to All Clients (Applica a tutti i client)***.
25. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Scheduled Scan Settings (Impostazioni per la scansione programmata)***.
26. Dal riquadro a sinistra, selezionare il collegamento ***Networked Computers (Computer in rete) > Client Management (Gestione client)***.
27. Sul lato destro, selezionare ***OfficeScan Server (Server OfficeScan)***.
28. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Scan Settings (Impostazioni scansione) > Scan Now Settings (Impostazioni per la scansione immediata)***. Viene visualizzata la schermata ***Scan Now Settings (Impostazioni per la scansione immediata)***.
29. Fare clic sulla scheda ***Target (Destinazione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
    - ***Scan Now Settings (Impostazioni per la scansione immediata) > Enable virus/malware scan (Attiva scansione virus/malware).***
    - ***Scan Now Settings (Impostazioni per la scansione immediata) > Enable spyware/grayware scan (Attiva scansione spyware/grayware).***
    - ***Files to Scan (File da analizzare) > File types scanned by IntelliScan (Tipi di file analizzati da IntelliScan).***
    - ***Scan Settings (Impostazioni scansione) > Scan compressed files (Analizza file compressi).***
    - ***Scan Settings (Impostazioni scansione) > Scan OLE objects (Analizza oggetti OLE).***
    - ***Virus/Malware Scan settings only (Solo impostazioni di scansione virus/malware) > Scan boot area (Analizza area di avvio).***
    - ***CPU Usage (Utilizzo CPU) > Low (Basso).***
    - ***Scan Exclusion (Esclusioni dalla scansione) > Enable scan exclusion (Attiva esclusioni dalla scansione).***
    - ***Scan Exclusion (Esclusioni dalla scansione) > Apply scan exclusion settings to all scan types (Applica impostazioni di esclusione dalla scansione a tutti i tipi di scansione).***

- ***Scan Exclusion List (Directories) (Elenco esclusioni dalla scansione (directory)) > Exclude directories where Trend Micro products are installed (Escludi directory in cui sono installati i prodotti Trend Micro).***
- Accertarsi che i percorsi delle cartelle ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** e ***G:*** siano presenti in Exclusion List (Elenco esclusioni).

30. Fare clic su ***Apply to All Clients (Applica a tutti i client)***.
31. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Scan now Settings (Impostazioni per la scansione immediata)***.
32. Dal riquadro a sinistra, selezionare il collegamento ***Networked Computers (Computer in rete) > Client Management (Gestione client)***.
33. Sul lato destro, selezionare ***OfficeScan Server (Server OfficeScan)***.
34. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Web Reputation Settings (Impostazioni reputazione Web)***. Viene visualizzata la schermata ***Web Reputation Settings (Impostazioni reputazione Web)***.
35. Fare clic sulla scheda ***External Clients (Client esterni)*** e deselezionare ***Enable Web reputation policy on the following operating systems (Attiva criterio di reputazione Web sui seguenti sistemi operativi)***, se l'opzione era già selezionata durante l'installazione.
36. Fare clic sulla scheda ***Internal Clients (Client interni)*** e deselezionare ***Enable Web reputation policy on the following operating systems (Attiva criterio di reputazione Web sui seguenti sistemi operativi)***, se l'opzione era già selezionata durante l'installazione.
37. Fare clic su ***Apply to All Clients (Applica a tutti i client)***.
38. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Web Reputation (Reputazione Web)***.
39. Dal riquadro a sinistra, selezionare il collegamento ***Networked Computers (Computer in rete) > Client Management (Gestione client)***.
40. Sul lato destro, selezionare ***OfficeScan Server (Server OfficeScan)***.
41. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Behavior Monitoring Settings (Impostazioni monitoraggio comportamento)***. Viene visualizzata la schermata ***Behavior Monitoring Settings (Impostazioni monitoraggio comportamento)***.
42. Deselezionare le opzioni ***Enable Malware Behavior Blocking (Attiva blocco comportamento malware)*** ed ***Enable Event Monitoring (Attiva monitoraggio eventi)***.
43. Fare clic su ***Apply to All Clients (Applica a tutti i client)***.
44. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Behavior Monitoring (Monitoraggio eventi)***.
45. Dal riquadro a sinistra, selezionare il collegamento ***Networked Computers (Computer in rete) > Client Management (Gestione client)***.
46. Sul lato destro, selezionare ***OfficeScan Server (Server OfficeScan)***.
47. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Device Control Settings (Impostazioni di controllo dispositivi)***. Viene visualizzata la schermata ***Device Control Settings (Impostazioni di controllo dispositivi)***.

48. Fare clic sulla scheda ***External Clients (Client esterni)*** e deselezionare le seguenti opzioni:
    - ***Notification (Notifica) > Display a notification message on the client computer when OfficeScan detects unauthorized device access (Visualizza un messaggio di notifica sul computer client quando OfficeScan rileva l'accesso di un dispositivo non autorizzato).***
    - ***Block the AutoRun function on USB storage devices (Blocca la funzione AutoRun sui dispositivi di memoria USB).***
    - ***Enable Device Control (Attiva controllo dispositivi).***
49. Fare clic sulla scheda ***Internal Clients (Client interni)*** e deselezionare le seguenti opzioni:
    - ***Notification (Notifica) > Display a notification message on the client computer when OfficeScan detects unauthorized device access (Visualizza un messaggio di notifica sul computer client quando OfficeScan rileva l'accesso di un dispositivo non autorizzato).***
    - ***Block the AutoRun function on USB storage devices (Blocca la funzione AutoRun sui dispositivi di memoria USB).***
    - ***Enable Device Control (Attiva controllo dispositivi).***
50. Fare clic su ***Apply to All Clients (Applica a tutti i client)***.
51. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Device Control Settings (Impostazioni di controllo dispositivi)***.
52. Dal riquadro a sinistra, selezionare il collegamento ***Networked Computers (Computer in rete) > Client Management (Gestione client)***.
53. Sul lato destro, selezionare ***OfficeScan Server (Server OfficeScan)***.
54. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Privileges and Other Settings (Privilegi e altre impostazioni)***.
55. Fare clic sulla scheda ***Privileges (Privilegi)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
    - ***Scan Privileges (Privilegi scansione) > Configure Manual Scan Settings (Configura impostazioni per la scansione manuale).***
    - ***Scan Privileges (Privilegi scansione) > Configure Real-time Scan Settings (Configura impostazioni di scansione in tempo reale).***
    - ***Scan Privileges (Privilegi scansione) > Configure Scheduled Scan Settings (Configura impostazioni per la scansione programmata).***
    - ***Proxy Setting Privileges (Privilegi impostazione proxy) > Allow the client user to configure proxy settings (Consenti all'utente client di configurare le impostazioni del proxy).***
    - ***Uninstallation (Disinstallazione) > Require a password for the user to uninstall the OfficeScan Client (Richiedi una password per la disinstallazione del client OfficeScan da parte dell'utente).*** Inserire una password idonea e confermarla.
    - ***Unloading (Scaricamento) > Require a password for the user to unload the OfficeScan client (Richiedi una password per lo scaricamento del client OfficeScan da parte dell'utente).*** Inserire una password idonea e confermarla.
56. Fare clic sulla scheda ***Other Settings (Altre impostazioni)***.
57. Selezionare ***Client Security Settings (Impostazioni di sicurezza del client) > Normal (Normale)*** e deselezionare le altre opzioni.

NOTA: È importante deselezionare le opzioni seguenti.

- ***Client Self-protection (Protezione automatica client) > Protect OfficeScan client services (Proteggi servizi client OfficeScan).***
- ***Client Self-protection (Protezione automatica client) > Protect files in the OfficeScan client installation folder (Proteggi i file nella cartella di installazione del client OfficeScan).***
- ***Client Self-protection (Protezione automatica client) > Protect OfficeScan client registry keys (Proteggi le chiavi di registro del client OfficeScan).***
- ***Client Self-protection (Protezione automatica client) > Protect OfficeScan client processes (Proteggi i processi del client OfficeScan).***

58. Fare clic su ***Apply to All Clients (Applica a tutti i client)***.
59. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Privileges and Other Settings (Privilegi e altre impostazioni)***.
60. Dal riquadro a sinistra, selezionare il collegamento ***Networked Computers (Computer in rete) > Client Management (Gestione client)***.
61. Sul lato destro, selezionare ***OfficeScan Server (Server OfficeScan)***.
62. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Additional Service Settings (Impostazioni servizi aggiuntivi)***.
63. Deselezionare l'opzione ***Enable service on the following operating systems (Attiva il servizio sui seguenti sistemi operativi)***.
64. Fare clic su ***Apply to All Clients (Applica a tutti i client)***.
65. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Additional Service Settings (Impostazioni servizi aggiuntivi)***.
66. Dal riquadro a sinistra, selezionare il collegamento ***Networked Computers (Computer in rete) > Global Client Settings (Impostazioni client globali)***.
67. Selezionare solo le seguenti opzioni, lasciando deselezionate le altre.

    - ***Scan Settings (Impostazioni scansione) > Configure Scan settings for large compressed files (Configura le impostazioni di scansione per i file compressi di grandi dimensioni).***
    - ***Scan Settings (Impostazioni scansione) > Do not scan files if the size exceeds 2 MB (Non analizzare i file di dimensioni superiori a 2 MB).***
    - ***Scan Settings (Impostazioni scansione) > In a compressed file scan only the first 100 files (Analizza solo i primi 100 file di un file compresso).***
    - ***Scan Settings (Impostazioni scansione) > Exclude the OfficeScan server database folder from Real-time Scan (Escludi la cartella del database del server OfficeScan dalla scansione in tempo reale).***
    - ***Scan Settings OfficeScan (Impostazioni scansione) > Exclude Microsoft Exchange server folders and files from scans (Escludi le cartelle e i file del server Microsoft Exchange dalle scansioni).***
    - ***Reserved Disk Space and Watchdog Settings (Impostazioni spazio su disco riservato e watchdog) > Reserve 60 MB of disk space for updates (Riserva 60 MB su disco per gli aggiornamenti).***
    - ***Proxy Configuration (Configurazione proxy) > Automatically detect settings (Rileva automaticamente impostazioni).***

NOTA: È importante deselezionare ***Alert Settings (Impostazioni avvisi) > Display a notification message if the client computer needs to restart to koad a kernel driver (Visualizza un messaggio di notifica se è necessario riavviare il computer client per caricare un driver del kernel)***.

68. Fare clic su ***Save (Salva)***.
69. Dal riquadro a sinistra, selezionare il collegamento ***Updates (Aggiornamenti) > Networked Computers (Computer in rete) > Manual Updates (Aggiornamenti manuali)***.
70. Selezionare ***Manually select client (Seleziona client manualmente)*** e fare clic su ***Select (Seleziona)***.
71. Fare clic sul nome di dominio appropriato in ***OfficeScan Server (Server OfficeScan)***.
72. Selezionare il sistema client, uno alla volta, e fare clic su ***Initiate Component Update (Avvia aggiornamento componenti)***.
73. Fare clic su ***OK*** nella finestra del messaggio.
74. Fare clic su ***Log off (Esci)*** e chiudere la console Web di OfficeScan.

Linee guida da seguire dopo l'installazione di Trend Micro OfficeScan

1. Nei sistemi di acquisizione, attenersi alla procedura seguente per configurare Trend Micro:
    a. Fare clic su ***Start > Control Panel (Pannello di controllo) > Network and Sharing Center (Centro connessioni di rete e condivisione)***.
    b. Fare clic su ***Change adapter settings (Modifica impostazioni scheda)***.
    c. Fare clic con il pulsante destro del mouse su ***Local Area Connection (Connessione alla rete locale)*** e selezionare ***Properties (Proprietà)***.
    d. Selezionare ***Internet Protocol Version 4 (TCP/IPv4) (Protocollo Internet versione 4 (TCP/IPv4)*** e fare clic su ***Properties (Proprietà)***.
    e. Registrare l'indirizzo IP _____.
    f. Chiudere tutte le finestre aperte.
    g. Fare clic su ***Start > Run (Esegui)*** e digitare **regedit**.
    h. Accedere a ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion***.
    i. Sul riquadro destro, fare clic con il pulsante destro del mouse su uno spazio vuoto e selezionare ***New > String value (Nuovo > Valore stringa)***.
    j. Per il nome digitare **IP Template (Modello IP)** e premere **Invio**.
    k. Fare doppio clic sulla voce del registro ***IP Template (Modello IP)***.
    l. Nel campo dati ***Value (Valore)***, inserire l'indirizzo IP di Local Area Connection (Connessione alla rete locale) registrato nel passaggio e.
    m. Fare clic su ***OK***.
    n. Chiudere l'editor del registro.

2. Attivare Loopback Connection (Connessione loopback). Per ulteriori informazioni, consultare Attivazione di Loopback Connection (Connessione loopback) a pagina 6.
3. Configurare il servizio Browser di computer. Per ulteriori informazioni, consultare Configurazione del servizio Browser di computer dopo l'installazione dell'antivirus a pagina 7.

Configurazioni delle impostazioni di Trend Micro Global

NOTA: Attenersi alle seguenti istruzioni quando si utilizza la funzione CO_2 con PDM nei sistemi Mac-Lab/CardioLab. Prima di effettuare la seguente procedura, esaminarla con il personale IT.

1. Sul server della console di gestione antivirus, accedere alla cartella ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV***.
2. Aprire il file ***ofcscan.ini*** in un editor di testo.
3. Nella sezione ***Global Setting (Impostazione globale)***, impostare "**1**" come valore della chiave seguente:
   [Impostazione globale] ***RmvTmTDI=1***
4. Salvare e chiudere il file ofcscan.ini.
5. Fare clic su ***Start > All Programs (Tutti i programmi) > Server TrendMicro OfficeScan - <server name> (<nome server>) > Console Web di OfficeScan***.
6. Inserire nome utente e password e fare clic su ***Log On (Accedi)***. Viene visualizzata la schermata ***Summary (Riepilogo)***.
7. Fare clic su ***Networked Computers (Computer in rete) > Global Client Settings (Impostazioni client globali)***.
8. Fare clic su ***Save (Salva)***.
9. Dal riquadro a sinistra, selezionare il collegamento ***Updates (Aggiornamenti) > Networked Computers (Computer in rete) > Manual Updates (Aggiornamento manuale)***.
10. Selezionare ***Manually select client (Seleziona client manualmente)*** e fare clic su ***Select (Seleziona)***.
11. Fare clic sul nome di dominio appropriato in ***OfficeScan Server (Server OfficeScan)***.
12. Selezionare il sistema client, uno alla volta, e fare clic su ***Initiate Component Update (Avvia aggiornamento componenti)***.
13. Fare clic su ***OK*** nella finestra del messaggio.
14. In ogni sistema di acquisizione, effettuare le seguenti operazioni:
    a. Aprire l'editor del registro.
    b. Accedere a ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc***.
    c. Accertarsi che il valore del registro ***RmvTmTDI*** sia impostato a "**1**".
    d. Accedere a ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.
    e. Eliminare la chiave di registro ***tmtdi***, se esiste.

f. Chiudere l'editor del registro.

g. Riavviare i sistemi client.

h. Accedere ai sistemi client come amministratore o come membro di tale gruppo.

i. Su ogni sistema client, aprire il prompt dei comandi con i privilegi di amministratore e inserire il comando "***sc query tmtdi***".

j. Accertarsi che venga visualizzato il messaggio ***The specified service does not exist as an installed service (Il servizio specificato non esiste come servizio installato)***.

15. Sul server della console di gestione antivirus, fare clic su ***Log off (Esci)*** e chiudere la console Web di OfficeScan.

Trend Micro OfficeScan Client/Server Edition 11.0 SP1

Installare Trend Micro OfficeScan Client/Server Edition solo in un ambiente di rete Mac-Lab/CardioLab. Trend Micro OfficeScan deve essere installato sul server della console di gestione antivirus e distribuito nel server Centricity Cardiology INW e nelle workstation di acquisizione/revisione come client. Attenersi alle seguenti istruzioni per installare ***Trend Micro OfficeScan Client/Server Edition 11.0 SP1***.

La responsabilità degli aggiornamenti antivirus spetta all'ospedale. Aggiornare regolarmente le definizioni, per assicurare che il sistema sia sempre protetto dai virus più recenti.

Linee guida da seguire prima dell'installazione

1. Si presuppone che la console di gestione antivirus di Trend Micro sia installata in base alle istruzioni di Trend Micro e che funzioni correttamente.
2. Durante l'installazione di Trend Micro OfficeScan, effettuare le seguenti operazioni sul server della console di gestione antivirus:
   a. Deselezionare ***Enable firewall (Attiva firewall)*** nella finestra ***Anti-virus Feature (Funzione antivirus)***.
   b. Selezionare ***No, Please do not enable assessment mode (Non attivare la modalità di valutazione)*** nella finestra ***Anti-spyware Feature (Funzione antispyware)***.
   c. Deselezionare ***Enable web reputation policy (Attiva criterio di reputazione Web)*** nella finestra ***Web Reputation Feature (Funzione reputazione Web)***.
3. Si sconsiglia di utilizzare Trend Micro OfficeScan assieme alla funzione CO_2 con PDM nei sistemi Mac-Lab/CardioLab.
4. Se Trend Micro OfficeScan è necessario:
   a. È preferibile configurare un server della console di gestione antivirus di Trend Micro separato per i sistemi Mac-Lab/CardioLab. È necessaria una modifica globale delle impostazioni antivirus per utilizzare la funzione CO_2 con PDM nei sistemi Mac-Lab/CardioLab.

b. Se non è possibile configurare un server della console di gestione antivirus di Trend Micro separato, è necessaria una modifica delle impostazioni globali del server della console di gestione antivirus di Trend Micro dopo l'installazione. Questa modifica riguarda tutti i sistemi client connessi al server della console di gestione antivirus di Trend Micro e deve essere esaminata con il personale IT prima di procedere.

5. Accedere come **Administrator (Amministratore)** o come membro di tale gruppo in tutti i sistemi client (acquisizione, revisione e server INW) per installare il software antivirus.
6. Disattivare Loopback Connection (Connessione loopback). Per ulteriori informazioni, consultare Disattivazione di Loopback Connection (Connessione loopback) a pagina 6.
7. Configurare il servizio Browser di computer. Per ulteriori informazioni, consultare Configurazione del servizio Browser di computer prima dell'installazione dell'antivirus a pagina 7.
8. Per l'installazione delle macchine client di acquisizione, revisione e server INW sono necessari i seguenti certificati di livello root e intermedio:
   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt
9. Ripetere i seguenti passaggi secondari per installare i cinque certificati di livello root e intermedio elencati nel passaggio 8.
   a. Accedere a ***C:\Program Files)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\EB***. NOTA: su INW, accedere a C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.
   b. Se il percorso della cartella indicato sopra non è presente, i certificati di livello root e intermedio necessari per l'installazione devono essere ottenuti manualmente.
   c. Fare doppio clic su ***AddTrustExternalCARoot.crt*** per installarlo sui sistemi MLCL (acquisizione, revisione e INW).
   d. Aprire il certificato e fare clic su ***Install Certificate (Installa certificato)***.
   e. Fare clic su ***Next (Avanti)*** quando appare ***Certificate Import Wizard (Importazione guidata certificati)***.
   f. Nella finestra ***Certificate Store (Archivio certificati)***, selezionare ***Place all certificates in the following store (Colloca tutti i certificati nel seguente archivio)*** e fare clic su ***Browse (Sfoglia)***.
   g. Selezionare ***Show physical stores > Trusted Root Certification Authorities > Local Computer (Mostra archivi fisici > Autorità di certificazione radice disponibile nell'elenco locale > Computer locale)*** e fare clic su ***OK***.
   h. Fare clic su ***Next (Avanti)*** in ***Certificate Import Wizard (Importazione guidata certificati)***.
   i. Fare clic su ***Finish (Fine)***. Dovrebbe essere visualizzato il messaggio ***The import was successful (Importazione completata)***.
   j. Ripetere il passaggio 9 per gli altri certificati elencati nel passaggio 8.

NOTA: Ogni certificato ha una propria data di scadenza. Per il corretto funzionamento delle funzioni dell'agente OfficeScan, i certificati scaduti devono essere rinnovati e aggiornati nei sistemi MLCL.

Trend Micro OfficeScan - Procedura di distribuzione di una nuova installazione (metodo di installazione push preferito per 11.0 SP1)

1. Fare clic su ***Start > All Programs (Tutti i programmi) > Server TrendMicro OfficeScan - <server name> (<nome server>) > Console Web di OfficeScan***.

NOTA: Continuare selezionando ***Continue with this website (Continuare con il sito Web) (Continuare con il sito Web (scelta non consigliata))***. Nella finestra Security Alert (Avviso di protezione), selezionare ***In the future, do not show this warning (Non mostrare l'avviso in futuro)*** e fare clic su ***OK***.

2. Se si ottiene un errore di certificato indicante che il sito non è attendibile, gestire i certificati includendo Trend Micro OfficeScan.
3. Se viene chiesto, installare i componenti aggiuntivi ***AtxEnc***. Viene visualizzata la schermata Security Warning (Avviso di protezione).
    a. Fare clic su ***Install (Installa)***
4. Inserire nome utente e password e fare clic su ***Log On (Accedi)***.
5. Se viene chiesto, fare clic su ***Update Now (Aggiorna ora)*** per installare nuovi widget. Attendere l'aggiornamento dei nuovi. Viene visualizzata la schermata indicante che l'aggiornamento è terminato.
    a. Fare clic su ***OK***.
6. Dalla barra dei menu superiore, fare clic su ***Agents (Agenti) > Agent Installation (Installazione agente) > Remote (Remota)***.
7. Se viene chiesto, installare i componenti aggiuntivi ***AtxConsole***. Viene visualizzata la schermata Security Warning (Avviso di protezione).
8. Fare doppio clic su ***OfficeScan Server (Server OfficeScan)*** nella finestra ***Remote Installation (Installazione remota)***. Vengono elencati tutti i domini in ***OfficeScan Server (Server OfficeScan)***.
9. Fare doppio clic sul dominio (ad esempio: INW) dall'elenco. Vengono visualizzati tutti i sistemi connessi al dominio.

NOTA: Se non vengono elencati né domini né sistemi nella finestra ***Domains and Endpoints (Domini ed endpoint)***, passare a Risoluzione dei problemi inerenti a domini o sistemi non elencati nella finestra Domains and Endpoints (Domini ed endpoint) a pagina 79 per aggiungerli manualmente o per eseguire l'installazione direttamente dalla macchina client.

10. Selezionare le macchine client (acquisizione, revisione e server INW) e fare clic su ***Add (Aggiungi)***.
11. Digitare <nome dominio>\nome utente e password e fare clic su ***Log on (Accedi)***.

12. Selezionare le macchine client (acquisizione, revisione e server INW), una alla volta, dal riquadro ***Selected Endpoints (Endpoint selezionati)*** e fare clic su ***Install (Installa)***.
13. Nella finestra di conferma, fare clic su ***OK***.
14. Fare clic su ***OK*** nella finestra del messaggio ***Number of clients to which notifications were sent (Numero di client a cui sono state inviate le notifiche)***.
15. Riavviare tutte le macchine client (acquisizione, revisione e server INW) e accedere come Administrator (Amministratore) o come membro di tale gruppo su tutte le macchine client, quindi attendere che l'icona di Trend Micro OfficeScan nella barra delle applicazioni diventi blu con un segno di spunta verde.
16. Fare clic sul collegamento ***Log Off (Esci)*** per chiudere la ***console Web di OfficeScan***.

Configurazione della console del server di Trend Micro OfficeScan per 11.0 SP1

1. Selezionare ***Start > All Programs (Tutti i programmi) > Server TrendMicro OfficeScan - <server name> (<nome server>) > OfficeScan Web Console (Console Web di OfficeScan)***. Viene visualizzata la schermata ***Trend Micro OfficeScan Login (Accesso a Trend Micro OfficeScan)***.
2. Inserire nome utente e password e fare clic su ***Login (Accedi)***. Viene visualizzata la schermata ***Summary (Riepilogo)***.
3. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.
4. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
5. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Scan Settings (Impostazioni scansione) > Manual Scan Settings (Impostazioni per la scansione manuale)***. Viene visualizzata la schermata ***Manual Scan Settings (Impostazioni per la scansione manuale)***.
6. Fare clic sulla scheda ***Target (Destinazione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
   - ***Files to Scan (File da analizzare) > File types scanned by IntelliScan (Tipi di file analizzati da IntelliScan).***
   - ***Scan Settings (Impostazioni scansione) > Scan compressed files (Analizza file compressi).***
   - ***Scan Settings (Impostazioni scansione) > Scan OLE objects (Analizza oggetti OLE).***
   - ***Virus/Malware Scan settings only (Solo impostazioni di scansione virus/malware) > Scan boot area (Analizza area di avvio).***
   - ***CPU Usage (Utilizzo CPU) > Low (Basso).***
7. Fare clic sulla scheda Scan Exclusion (Esclusione scansione) e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
   - ***Scan Exclusion (Esclusioni dalla scansione) > Enable scan exclusion (Attiva esclusioni dalla scansione).***
   - ***Scan Exclusion (Esclusioni dalla scansione) > Apply scan exclusion settings to all scan types (Applica impostazioni di esclusione dalla scansione a tutti i tipi di scansione).***

- ***Scan Exclusion List (Directories) (Elenco esclusioni dalla scansione (directory)) > Exclude directories where Trend Micro products are installed (Escludi directory in cui sono installati i prodotti Trend Micro).***
- Selezionare ***Adds path (Percorso aggiunta)*** dall'elenco a discesa in ***Saving the officescan agent's exclusion list does the following: (Il salvataggio dell'elenco esclusioni degli agenti OfficeScan comporta le seguenti operazioni:)***
- Inserire le cartelle **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:** e **G:**, una alla volta, e fare clic su **+**.

8. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
9. Fare clic su ***OK*** nel messaggio ***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier. Do you want to proceed? (L'elenco esclusioni in questa schermata sostituirà quello nei client o nei domini selezionati precedentemente nella struttura client. Procedere?)***.
10. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Manual Scan Settings (Impostazioni per la scansione manuale)***.
11. Dal riquadro superiore, selezionare il collegamento ***Agent (Agente) > Agent Management (Gestione agenti)***.
12. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
13. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Scan Settings (Impostazioni scansione) > Real-time Scan Settings (Impostazioni di scansione in tempo reale)***. Viene visualizzata la schermata ***Real-time Scan Settings (Impostazioni di scansione in tempo reale)***.
14. Fare clic sulla scheda ***Target (Destinazione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
    - ***Real-Time Scan Settings (Impostazioni di scansione in tempo reale) > Enable virus/malware scan (Attiva scansione virus/malware).***
    - ***Real-Time Scan Settings (Impostazioni di scansione in tempo reale) > Enable spyware/grayware scan (Attiva scansione spyware/grayware).***
    - ***Files to Scan (File da analizzare) > File types scanned by IntelliScan (Tipi di file analizzati da IntelliScan).***
    - ***Scan Settings (Impostazioni scansione) > Scan compressed files (Analizza file compressi).***
    - ***Scan Settings (Impostazioni scansione) > Scan OLE objects (Analizza oggetti OLE).***
    - ***Virus/Malware Scan Settings Only (Solo impostazioni di scansione virus/malware) > Enable IntelliTrap (Attiva IntelliTrap).***
15. Fare clic sulla scheda Scan Exclusion (Esclusione scansione) e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
    - ***Scan Exclusion (Esclusioni dalla scansione) > Enable scan exclusion (Attiva esclusioni dalla scansione).***
    - ***Scan Exclusion (Esclusioni dalla scansione) > Apply scan exclusion settings to all scan types (Applica impostazioni di esclusione dalla scansione a tutti i tipi di scansione).***
    - ***Scan Exclusion List (Directories) (Elenco esclusioni dalla scansione (directory)) > Exclude directories where Trend Micro products are installed (Escludi directory in cui sono installati i prodotti Trend Micro).***

- Accertarsi che i percorsi delle cartelle ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** e ***G:*** siano presenti in ***Exclusion List (Elenco esclusioni)***.

16. Fare clic sulla scheda ***Action (Azione)***.
17. Lasciare le impostazioni predefinite e deselezionare le seguenti opzioni:
    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected (Visualizza un messaggio di notifica sugli endpoint al rilevamento di virus/malware).***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected (Visualizza un messaggio di notifica sugli endpoint al rilevamento di spyware/grayware).***
18. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
19. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Real-time Scan Settings (Impostazioni di scansione in tempo reale)***.
20. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.
21. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
22. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Scan Settings (Impostazioni scansione) > Scheduled Scan Settings (Impostazioni per la scansione programmata)***. Viene visualizzata la schermata ***Scheduled Scan Settings (Impostazioni per la scansione programmata)***.
23. Fare clic sulla scheda ***Target (Destinazione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
    - ***Scheduled Scan Settings (Impostazioni per la scansione programmata) > Enable virus/malware scan (Attiva scansione virus/malware).***
    - ***Scheduled Scan Settings (Impostazioni per la scansione programmata) > Enable spyware/grayware scan (Attiva scansione spyware/grayware).***
    - ***Schedule (Programmazione) > Weekly, every Sunday, Start time: 00:00 hh:mm (Settimanale, ogni domenica, ora di inizio: 00:00 hh:mm).***
    - ***Files to Scan (File da analizzare) > File types scanned by IntelliScan (Tipi di file analizzati da IntelliScan).***
    - ***Scan Settings (Impostazioni scansione) > Scan compressed files (Analizza file compressi).***
    - ***Scan Settings (Impostazioni scansione) > Scan OLE objects (Analizza oggetti OLE).***
    - ***Virus/Malware Scan settings only (Solo impostazioni di scansione virus/malware) > Scan boot area (Analizza area di avvio).***
    - ***CPU Usage (Utilizzo CPU) > Low (Basso).***
24. Fare clic sulla scheda ***Scan Exclusion (Esclusione scansione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
    - ***Scan Exclusion (Esclusioni dalla scansione) > Enable scan exclusion (Attiva esclusioni dalla scansione).***
    - ***Scan Exclusion (Esclusioni dalla scansione) > Apply scan exclusion settings to all scan types (Applica impostazioni di esclusione dalla scansione a tutti i tipi di scansione).***

- ***Scan Exclusion List (Directories) (Elenco esclusioni dalla scansione (directory)) > Exclude directories where Trend Micro products are installed (Escludi directory in cui sono installati i prodotti Trend Micro).***
- Accertarsi che i percorsi delle cartelle ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** e ***G:*** siano presenti in Exclusion List (Elenco esclusioni).

25. Fare clic sulla scheda ***Action (Azione)***.
26. Lasciare le impostazioni predefinite e deselezionare le seguenti opzioni:
    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected (Visualizza un messaggio di notifica sugli endpoint al rilevamento di virus/malware).***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected (Visualizza un messaggio di notifica sugli endpoint al rilevamento di spyware/grayware).***
27. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
28. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Scheduled Scan Settings (Impostazioni per la scansione programmata)***.
29. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.
30. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
31. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Scan Settings (Impostazioni scansione) > Scan Now Settings (Impostazioni per la scansione immediata)***. Viene visualizzata la schermata ***Scan Now Settings (Impostazioni per la scansione immediata)***.
32. Fare clic sulla scheda ***Target (Destinazione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
    - ***Scan Now Settings (Impostazioni per la scansione immediata) > Enable virus/malware scan (Attiva scansione virus/malware).***
    - ***Scan Now Settings (Impostazioni per la scansione immediata) > Enable spyware/grayware scan (Attiva scansione spyware/grayware).***
    - ***Files to Scan (File da analizzare) > File types scanned by IntelliScan (Tipi di file analizzati da IntelliScan).***
    - ***Scan Settings (Impostazioni scansione) > Scan compressed files (Analizza file compressi).***
    - ***Scan Settings (Impostazioni scansione) > Scan OLE objects (Analizza oggetti OLE).***
    - ***Virus/Malware Scan settings only (Solo impostazioni di scansione virus/malware) > Scan boot area (Analizza area di avvio).***
    - ***CPU Usage (Utilizzo CPU) > Low (Basso).***
33. Fare clic sulla scheda ***Scan Exclusion (Esclusione scansione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
    - ***Scan Exclusion (Esclusioni dalla scansione) > Enable scan exclusion (Attiva esclusioni dalla scansione).***
    - ***Scan Exclusion (Esclusioni dalla scansione) > Apply scan exclusion settings to all scan types (Applica impostazioni di esclusione dalla scansione a tutti i tipi di scansione).***

- ***Scan Exclusion List (Directories) (Elenco esclusioni dalla scansione (directory)) > Exclude directories where Trend Micro products are installed (Escludi directory in cui sono installati i prodotti Trend Micro).***
- Accertarsi che i percorsi delle cartelle ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** e ***G:*** siano presenti in Exclusion List (Elenco esclusioni).

34. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
35. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Scan now Settings (Impostazioni per la scansione immediata)***.
36. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.
37. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
38. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Web Reputation Settings (Impostazioni reputazione Web)***. Viene visualizzata la schermata ***Web Reputation Settings (Impostazioni reputazione Web)***.
39. Fare clic sulla scheda ***External Agents (Agenti esterni)*** e deselezionare ***Enable Web reputation policy on the following operating systems (Attiva criterio di reputazione Web sui seguenti sistemi operativi)***, se l'opzione era già selezionata durante l'installazione.
40. Fare clic sulla scheda ***Internal Agents (Agenti interni)*** e deselezionare ***Enable Web reputation policy on the following operating systems (Attiva criterio di reputazione Web sui seguenti sistemi operativi)***, se l'opzione era già selezionata durante l'installazione.
41. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
42. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Web Reputation (Reputazione Web)***.
43. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.
44. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
45. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Behavior Monitoring Settings (Impostazioni monitoraggio comportamento)***. Viene visualizzata la schermata ***Behavior Monitoring Settings (Impostazioni monitoraggio comportamento)***.
46. Deselezionare le opzioni ***Enable Malware Behavior Blocking for known and potential threats (attiva blocco comportamento malware per minacce note e potenziali)*** e ***Enable Event Monitoring (Attiva monitoraggio eventi)***.
47. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
48. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Behavior Monitoring (Monitoraggio eventi)***.
49. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.
50. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
51. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Device Control Settings (Impostazioni di controllo dispositivi)***. Viene visualizzata la schermata ***Device Control Settings (Impostazioni di controllo dispositivi)***.

52. Fare clic sulla scheda ***External Agents (Agenti esterni)*** e deselezionare le seguenti opzioni:
    - ***Notification (Notifica) > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Visualizza un messaggio di notifica sugli endpoint quando OfficeScan rileva l'accesso di un dispositivo non autorizzato).***
    - ***Block the AutoRun function on USB storage devices (Blocca la funzione AutoRun sui dispositivi di memoria USB).***
53. Fare clic sulla scheda ***Internal Agents (Agenti interni)*** e deselezionare le seguenti opzioni:
    - ***Notification (Notifica) > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Visualizza un messaggio di notifica sugli endpoint quando OfficeScan rileva l'accesso di un dispositivo non autorizzato).***
    - ***Block the AutoRun function on USB storage devices (Blocca la funzione AutoRun sui dispositivi di memoria USB).***
54. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
55. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Device Control Settings (Impostazioni di controllo dispositivi)***.
56. Dalle opzioni ***Settings (Impostazioni)***, selezionare nuovamente ***Device Control Settings (Impostazioni di controllo dispositivi)***. Viene visualizzata la schermata ***Device Control Settings (Impostazioni di controllo dispositivi)***.
57. Fare clic sulla scheda ***External Agents (Agenti esterni)*** e deselezionare ***Enable Device Control (Attiva controllo dispositivi)***.
58. Fare clic sulla scheda ***Internal Agents (Agenti interni)*** e deselezionare ***Enable Device Control (Attiva controllo dispositivi)***.
59. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
60. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Device Control Settings (Impostazioni di controllo dispositivi)***.
61. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.
62. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
63. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Privileges and Other Settings (Privilegi e altre impostazioni)***.
64. Fare clic sulla scheda ***Privileges (Privilegi)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
    - ***Scans (Scansioni) > Configure Manual Scan Settings (Configura impostazioni per la scansione manuale).***
    - ***Scans (Scansioni) > Configure Real-time Scan Settings (Configura impostazioni di scansione in tempo reale).***
    - ***Scans (Scansioni) > Configure Scheduled Scan Settings (Configura impostazioni per la scansione programmata).***
    - ***Proxy Setting (Impostazioni proxy) > Allow users to configure proxy settings (Consenti agli utenti di configurare le impostazioni del proxy).***

- ***Uninstallation (Disinstallazione) > Requires a password (Richiede una password).*** Inserire una password idonea e confermarla.
- ***Unloading and Unlock (Scarica e sblocca) > Requires a password > (Richiede una password).*** Inserire una password idonea e confermarla.

65. Fare clic sulla scheda ***Other Settings (Altre impostazioni)***.
66. Selezionare ***OfficeScan Agent Security Settings (Impostazioni di protezione agente OfficeScan) > Normal: Allow users to access OfficeScan agent files and registries (Normale: consenti agli utenti di accedere a file e registri dell'agent OfficeScan)*** e deselezionare le opzioni rimanenti.

NOTA: È importante deselezionare le opzioni seguenti.

- ***OfficeScan Agent Self-protection (Protezione automatica agente OfficeScan) > Protect OfficeScan agent services (Proteggi servizi agente OfficeScan).***
- ***OfficeScan Agent Self-protection (Protezione automatica agente OfficeScan) > Protect files in the OfficeScan agent installation folder (Proteggi i file nella cartella di installazione dell'agente OfficeScan).***
- ***OfficeScan Agent Self-protection (Protezione automatica agente OfficeScan) > Protect OfficeScan agent registry keys (Proteggi chiavi di registro agente OfficeScan).***
- ***OfficeScan Agent Self-protection (Protezione automatica agente OfficeScan) > Protect OfficeScan agent processes (Proteggi processi agente OfficeScan).***

67. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
68. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Privileges and Other Settings (Privilegi e altre impostazioni)***.
69. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.
70. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
71. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Additional Service Settings (Impostazioni servizi aggiuntivi)***.
72. Deselezionare l'opzione ***Enable service on the following operating systems (Attiva il servizio sui seguenti sistemi operativi)***.
73. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
74. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Additional Service Settings (Impostazioni servizi aggiuntivi)***.
75. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Global Agent Settings (Impostazioni globali agenti)***.
76. Selezionare solo le seguenti opzioni, lasciando deselezionate le altre.

- ***Scan Settings for Large Compressed Files (Impostazioni scansione per i file compressi di grandi dimensioni) > Configure Scan settings for large compressed files (Configura le impostazioni di scansione per i file compressi di grandi dimensioni).***

- ***Scan Settings for Large Compressed Files (Impostazioni scansione per i file compressi di grandi dimensioni) > Do not scan files if the size exceeds 2 MB (Non analizzare i file di dimensioni superiori a 2 MB)***. Effettuare queste operazioni per ***Real-Time Scan (Scansione in tempo reale)*** e ***Manual Scan (Scansione manuale) / Schedule Scan (Scansione programmata) / Scan Now (Scansione immediata)***.
- ***Scan Settings for Large Compressed Files (Impostazioni scansione per i file compressi di grandi dimensioni) > In a compressed file scan only the first 100 files (Analizza solo i primi 100 file di un file compresso).*** Effettuare queste operazioni per ***Real-Time Scan (Scansione in tempo reale)*** e ***Manual Scan (Scansione manuale) / Schedule Scan (Scansione programmata) / Scan Now (Scansione immediata)***.
- ***Scan Settings (Impostazioni scansione) > Exclude the OfficeScan server database folder from Real-time Scan (Escludi la cartella del database del server OfficeScan dalla scansione in tempo reale).***
- ***Scan Settings OfficeScan (Impostazioni scansione) > Exclude Microsoft Exchange server folders and files from scans (Escludi le cartelle e i file del server Microsoft Exchange dalle scansioni).***
- ***Reserved Disk Space and Watchdog Settings (Impostazioni spazio su disco riservato e watchdog) > Reserve 60 MB of disk space for updates (Riserva 60 MB su disco per gli aggiornamenti).***
- ***Proxy Configuration (Configurazione proxy) > Automatically detect settings (Rileva automaticamente impostazioni).***

NOTA: È importante deselezionare ***Alert Settings (Impostazioni avvisi) > Display a notification message if the endpoint needs to restart to load a Kernel mode driver (Visualizza un messaggio di notifica se è necessario riavviare l'endpoint per caricare un driver in modalità kernel)***.

77. Fare clic su ***Save (Salva)***.
78. Dal riquadro superiore, selezionare il collegamento ***Updates (Aggiornamenti) > Agents (Agenti) > Manual Updates (Aggiornamenti manuali)***.
79. Selezionare ***Manually select agents (Seleziona agenti manualmente)*** e fare clic su ***Select (Seleziona)***.
80. Fare doppio clic sul nome di dominio appropriato in ***OfficeScan Server (Server OfficeScan)***.
81. Selezionare il sistema client, uno alla volta, e fare clic su ***Initiate Update (Avvia aggiornamento)***.
82. Fare clic su ***OK*** nella finestra del messaggio.
83. Fare clic su ***Log off (Esci)*** e chiudere la console Web di OfficeScan.

Configurazioni delle impostazioni di Trend Micro Global

NOTA: Attenersi alle seguenti istruzioni quando si utilizza la funzione CO_2 con PDM nei sistemi Mac-Lab/CardioLab. Prima di effettuare la seguente procedura, esaminarla con il personale IT.

1. Sul server della console di gestione antivirus, accedere alla cartella ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV***.
2. Aprire il file ***ofcscan.ini*** in un editor di testo.
3. Nella sezione Impostazione globale, impostare "**1**" come valore della chiave seguente: [Impostazione globale] ***RmvTmTDI=1***

4. Salvare e chiudere il file ofcscan.ini.
5. Fare clic su ***Start > All Programs (Tutti i programmi) > Server TrendMicro OfficeScan - <server name> (<nome server>) > Console Web di OfficeScan***.
6. Inserire nome utente e password e fare clic su ***Log On (Accedi)***. Viene visualizzata la schermata ***Dashboard***.
7. Fare clic su ***Agents (Agenti) > Global Agent Settings (Impostazioni globali agenti)***.
8. Fare clic su ***Save (Salva)***.
9. Dal riquadro a sinistra, selezionare il collegamento ***Updates (Aggiornamenti) > Agents (Agenti) > Manual Update (Aggiornamento manuale)***.
10. Selezionare ***Manually select clients (Seleziona client manualmente)*** e fare clic su ***Select (Seleziona)***.
11. Fare clic sul nome di dominio appropriato in ***OfficeScan Server (Server OfficeScan)***.
12. Selezionare il sistema client, uno alla volta, e fare clic su ***Initiate Update (Avvia aggiornamento)***.
13. Fare clic su ***OK*** nella finestra del messaggio.
14. In ogni sistema di acquisizione, effettuare le seguenti operazioni:
    a. Aprire l'editor del registro.
    b. Accedere a ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc.***
    c. Accertarsi che il valore del registro ***RmvTmTDI*** sia impostato a "***1***".
    d. Accedere a ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.
    e. Eliminare la chiave di registro ***tmtdi***, se esiste.
    f. Chiudere l'editor del registro.
    g. Riavviare i sistemi client.
    h. Accedere ai sistemi client come amministratore o come membro di tale gruppo.
    i. Su ogni sistema client, aprire il prompt dei comandi con i privilegi di amministratore e inserire il comando "***sc query tmtdi***".
    j. Accertarsi che venga visualizzato il messaggio ***The specified service does not exist as an installed service (Il servizio specificato non esiste come servizio installato)***.
15. Sul server della console di gestione antivirus, fare clic su ***Log off (Esci)*** e chiudere la console Web di OfficeScan.

Linee guida da seguire dopo l'installazione di Trend Micro OfficeScan

1. Attivare Loopback Connection (Connessione loopback). Per ulteriori informazioni, consultare Attivazione di Loopback Connection (Connessione loopback) a pagina 6.

2. Configurare il servizio Browser di computer. Per ulteriori informazioni, consultare Configurazione del servizio Browser di computer dopo l'installazione dell'antivirus a pagina 7.

Trend Micro OfficeScan Client/Server Edition XG 12.0

Panoramica dell'installazione

Installare Trend Micro OfficeScan Client/Server Edition solo in un ambiente di rete Mac-Lab/CardioLab. Trend Micro OfficeScan deve essere installato sul server della console di gestione antivirus e distribuito nel server Centricity Cardiology INW e nelle workstation di acquisizione/revisione come client. Attenersi alle seguenti istruzioni per installare ***Trend Micro OfficeScan Client/Server Edition XG 12.0***.

La responsabilità degli aggiornamenti antivirus spetta all'ospedale. Aggiornare regolarmente le definizioni, per assicurare che il sistema sia sempre protetto dai virus più recenti.

Linee guida da seguire prima dell'installazione

NOTA: Per l'esecuzione del gestore OfficeScan, come browser è necessario Internet Explorer 10 (o versioni più recenti).

1. Si presuppone che la console di gestione antivirus di Trend Micro sia installata in base alle istruzioni di Trend Micro e che funzioni correttamente.
2. Durante l'installazione di Trend Micro OfficeScan, effettuare le seguenti operazioni sul server della console di gestione antivirus:
   a. Deselezionare ***Enable firewall (Attiva firewall)*** nella finestra ***Anti-virus Feature (Funzione antivirus)***.
   b. Selezionare ***No, Please do not enable assessment mode (Non attivare la modalità di valutazione)*** nella finestra ***Anti-spyware Feature (Funzione antispyware)***.
   c. Deselezionare ***Enable web reputation policy (Attiva criterio di reputazione Web)*** nella finestra ***Web Reputation Feature (Funzione reputazione Web)***.
3. Accedere come **Administrator (Amministratore)** o come membro di tale gruppo in tutti i sistemi client (acquisizione, revisione e server INW) per installare il software antivirus.
4. Disattivare Loopback Connection (Connessione loopback). Per ulteriori informazioni, consultare Disattivazione di Loopback Connection (Connessione loopback) a pagina 6.
5. Configurare il servizio Browser di computer. Per ulteriori informazioni, consultare Configurazione del servizio Browser di computer prima dell'installazione dell'antivirus a pagina 7.
6. Per l'installazione delle macchine client di acquisizione, revisione e server INW sono necessari i seguenti certificati di livello root e intermedio:
   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt

7. Ripetere i seguenti passaggi secondari per installare i cinque certificati di livello root e intermedio elencati nel passaggio 6.

    a. Accedere a ***C:\Program Files)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\EB***. NOTA: su INW, accedere a C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.

    b. Se il percorso della cartella indicato sopra non è presente, i certificati di livello root e intermedio necessari per l'installazione devono essere ottenuti manualmente.

    c. Fare doppio clic su ***AddTrustExternalCARoot.crt*** per installarlo sui sistemi MLCL (acquisizione, revisione e INW).

    d. Aprire il certificato e fare clic su ***Install Certificate (Installa certificato)***.

    e. Fare clic su ***Next (Avanti)*** quando appare ***Certificate Import Wizard (Importazione guidata certificati)***.

    f. Nella finestra ***Certificate Store (Archivio certificati)***, selezionare ***Place all certificates in the following store (Colloca tutti i certificati nel seguente archivio)*** e fare clic su ***Browse (Sfoglia)***.

    g. Selezionare ***Show physical stores > Trusted Root Certification Authorities > Local Computer (Mostra archivi fisici > Autorità di certificazione radice disponibile nell'elenco locale > Computer locale)*** e fare clic su ***OK***.

    h. Fare clic su ***Next (Avanti)*** in ***Certificate Import Wizard (Importazione guidata certificati)***.

    i. Fare clic su ***Finish (Fine)***. Dovrebbe essere visualizzato il messaggio ***The import was successful (Importazione completata)***.

    j. Ripetere il passaggio 7 per gli altri certificati elencati nel passaggio 6.

NOTA: Ogni certificato ha una propria data di scadenza. Per il corretto funzionamento delle funzioni dell'agente OfficeScan, i certificati scaduti devono essere rinnovati e aggiornati nei sistemi MLCL.

Trend Micro OfficeScan - Procedura di distribuzione di una nuova installazione (metodo di installazione push preferito per 12.0)

1. Fare clic su ***Start > All Programs (Tutti i programmi) > Server TrendMicro OfficeScan - <server name> (<nome server>) > Console Web di OfficeScan***.

NOTA: Continuare selezionando ***Continue with this website (Continuare con il sito Web) (Continuare con il sito Web (scelta non consigliata))***. Nella finestra Security Alert (Avviso di protezione), selezionare ***In the future, do not show this warning (Non mostrare l'avviso in futuro)*** e fare clic su ***OK***.

2. Se si ottiene un errore di certificato indicante che il sito non è attendibile, gestire i certificati includendo Trend Micro OfficeScan.

3. Se viene chiesto, installare i componenti aggiuntivi ***AtxEnc***. Viene visualizzata la schermata Security Warning (Avviso di protezione).

    a. Fare clic su ***Install (Installa)***

4. Inserire nome utente e password e fare clic su ***Log On (Accedi)***.

5. Se viene chiesto, fare clic su ***Update Now (Aggiorna ora)*** per installare nuovi widget. Attendere l'aggiornamento dei nuovi. Viene visualizzata la schermata indicante che l'aggiornamento è terminato.

   a. Fare clic su ***OK***.

6. Dalla barra dei menu superiore, fare clic su ***Agents (Agenti) > Agent Installation (Installazione agente) > Remote (Remota)***.

7. Se viene chiesto, installare i componenti aggiuntivi ***AtxConsole***. Viene visualizzata la schermata Security Warning (Avviso di protezione).

   a. Fare clic su ***Install (Installa)***.

8. Fare doppio clic su ***My Company (La mia azienda)*** nella finestra ***Remote Installation (Installazione remota)***. Vengono elencati tutti i domini in ***OfficeScan Server (Server OfficeScan)***.

9. Fare doppio clic sul dominio (ad esempio: INW) dall'elenco. Vengono visualizzati tutti i sistemi connessi al dominio.

NOTA: Se non vengono elencati né domini né sistemi nella finestra ***Domains and Endpoints (Domini ed endpoint)***, passare a Risoluzione dei problemi inerenti a domini o sistemi non elencati nella finestra Domains and Endpoints (Domini ed endpoint) a pagina 79 per aggiungerli manualmente o per eseguire l'installazione direttamente dalla macchina client.

10. Selezionare le macchine client (acquisizione, revisione e server INW) e fare clic su ***Add (Aggiungi)***.

11. Digitare <nome dominio>\nome utente e password e fare clic su ***Log on (Accedi)***.

12. Selezionare le macchine client (acquisizione, revisione e server INW), una alla volta, dal riquadro ***Selected Endpoints (Endpoint selezionati)*** e fare clic su ***Install (Installa)***.

13. Fare clic su ***Yes (Si)*** nella finestra di conferma.

14. Fare clic su ***OK*** nella finestra del messaggio ***Number of agents to which notifications were sent (Numero di agenti a cui sono state inviate le notifiche)***.

15. Riavviare tutte le macchine client (acquisizione, revisione e server INW) e accedere come Administrator (Amministratore) o come membro di tale gruppo su tutte le macchine client, quindi attendere che l'icona di Trend Micro OfficeScan nella barra delle applicazioni diventi blu con un segno di spunta verde.

16. Fare clic sul collegamento ***Log Off (Esci)*** per chiudere la ***console Web di OfficeScan***.

Configurazione della console del server di Trend Micro OfficeScan per 12.0

1. Selezionare ***Start > All Programs (Tutti i programmi) > Server TrendMicro OfficeScan - <server name> (<nome server>) > OfficeScan Web Console (Console Web di OfficeScan)***. Viene visualizzata la schermata ***Trend Micro OfficeScan Login (Accesso a Trend Micro OfficeScan)***.

2. Inserire nome utente e password e fare clic su ***Login (Accedi)***. Viene visualizzata la schermata ***Summary (Riepilogo)***.

3. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.
4. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
5. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Scan Settings (Impostazioni scansione) > Manual Scan Settings (Impostazioni per la scansione manuale)***. Viene visualizzata la schermata ***Manual Scan Settings (Impostazioni per la scansione manuale)***.
6. Fare clic sulla scheda ***Target (Destinazione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
   - ***Files to Scan (File da analizzare) > File types scanned by IntelliScan (Tipi di file analizzati da IntelliScan).***
   - ***Scan Settings (Impostazioni scansione) > Scan compressed files (Analizza file compressi).***
   - ***Scan Settings (Impostazioni scansione) > Scan OLE objects (Analizza oggetti OLE).***
   - ***Virus/Malware Scan settings only (Solo impostazioni di scansione virus/malware) > Scan boot area (Analizza area di avvio).***
   - ***CPU Usage (Utilizzo CPU) > Low (Basso).***
7. Fare clic sulla scheda Scan Exclusion (Esclusione scansione) e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
   - ***Scan Exclusion (Esclusioni dalla scansione) > Enable scan exclusion (Attiva esclusioni dalla scansione).***
   - ***Scan Exclusion (Esclusioni dalla scansione) > Apply scan exclusion settings to all scan types (Applica impostazioni di esclusione dalla scansione a tutti i tipi di scansione).***
   - ***Scan Exclusion List (Directories) (Elenco esclusioni dalla scansione (directory)) > Exclude directories where Trend Micro products are installed and select Add path to agent Computers Exclusion list (Escludi directory in cui sono installati i prodotti Trend Micro e seleziona percorso di aggiunta all'elenco di esclusione dei computer degli agenti).***
   - Selezionare ***Adds path (Percorso aggiunta)*** dall'elenco a discesa in ***Saving the officescan agent's exclusion list does the following: (Il salvataggio dell'elenco esclusioni degli agenti OfficeScan comporta le seguenti operazioni:)***
   - Inserire le cartelle **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL, D:\GEData\Studies**, **E:** e **G:**, una alla volta, e fare clic su ***Add (Aggiungi)***.
8. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
9. Fare clic su ***OK*** nel messaggio ***The exclusion list on this screen will replace the exclusion list on the agents or domains you selected in the client tree earlier. Do you want to proceed? (L'elenco esclusioni in questa schermata sostituirà quello nei client o nei domini selezionati precedentemente nella struttura client. Procedere?)***.
10. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Manual Scan Settings (Impostazioni per la scansione manuale)***.
11. Dal riquadro superiore, selezionare il collegamento ***Agent (Agente) > Agent Management (Gestione agenti)***.
12. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.

13. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Scan Settings (Impostazioni scansione) > Real-time Scan Settings (Impostazioni di scansione in tempo reale)***. Viene visualizzata la schermata ***Real-time Scan Settings (Impostazioni di scansione in tempo reale)***.

14. Fare clic sulla scheda ***Target (Destinazione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:

    - ***Real-Time Scan Settings (Impostazioni di scansione in tempo reale) > Enable virus/malware scan (Attiva scansione virus/malware).***
    - ***Real-Time Scan Settings (Impostazioni di scansione in tempo reale) > Enable spyware/grayware scan (Attiva scansione spyware/grayware).***
    - ***Files to Scan (File da analizzare) > File types scanned by IntelliScan (Tipi di file analizzati da IntelliScan).***
    - ***Scan Settings (Impostazioni scansione) > Scan compressed files (Analizza file compressi).***
    - ***Scan Settings (Impostazioni scansione) > Scan OLE objects (Analizza oggetti OLE).***
    - ***Virus/Malware Scan Settings Only (Solo impostazioni di scansione virus/malware) > Enable IntelliTrap (Attiva IntelliTrap).***

15. Fare clic sulla scheda Scan Exclusion (Esclusione scansione) e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:

    - ***Scan Exclusion (Esclusioni dalla scansione) > Enable scan exclusion (Attiva esclusioni dalla scansione).***
    - ***Scan Exclusion (Esclusioni dalla scansione) > Apply scan exclusion settings to all scan types (Applica impostazioni di esclusione dalla scansione a tutti i tipi di scansione).***
    - ***Scan Exclusion List (Directories) (Elenco esclusioni dalla scansione (directory)) > Exclude directories where Trend Micro products are installed (Escludi directory in cui sono installati i prodotti Trend Micro).***
    - Accertarsi che i percorsi delle cartelle ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:*** e ***G:*** siano presenti in ***Exclusion List (Elenco esclusioni)***.

16. Fare clic sulla scheda ***Action (Azione)***.

17. Lasciare le impostazioni predefinite e deselezionare le seguenti opzioni:

    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected (Visualizza un messaggio di notifica sugli endpoint al rilevamento di virus/malware).***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected (Visualizza un messaggio di notifica sugli endpoint al rilevamento di spyware/grayware).***

18. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.

19. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Real-time Scan Settings (Impostazioni di scansione in tempo reale)***.

20. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.

21. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.

22. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Scan Settings (Impostazioni scansione) > Scheduled Scan Settings (Impostazioni per la scansione programmata)***. Viene visualizzata la schermata ***Scheduled Scan Settings (Impostazioni per la scansione programmata)***.

23. Fare clic sulla scheda ***Target (Destinazione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:

    - ***Scheduled Scan Settings (Impostazioni per la scansione programmata) > Enable virus/malware scan (Attiva scansione virus/malware).***
    - ***Scheduled Scan Settings (Impostazioni per la scansione programmata) > Enable spyware/grayware scan (Attiva scansione spyware/grayware).***
    - ***Schedule (Programmazione) > Weekly, every Sunday, Start time: 00:00 hh:mm (Settimanale, ogni domenica, ora di inizio: 00:00 hh:mm).***
    - ***Files to Scan (File da analizzare) > File types scanned by IntelliScan (Tipi di file analizzati da IntelliScan).***
    - ***Scan Settings (Impostazioni scansione) > Scan compressed files (Analizza file compressi).***
    - ***Scan Settings (Impostazioni scansione) > Scan OLE objects (Analizza oggetti OLE).***
    - ***Virus/Malware Scan settings only (Solo impostazioni di scansione virus/malware) > Scan boot area (Analizza area di avvio).***
    - ***CPU Usage (Utilizzo CPU) > Low (Basso).***

24. Fare clic sulla scheda Scan Exclusion (Esclusione scansione) e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:

    - ***Scan Exclusion (Esclusioni dalla scansione) > Enable scan exclusion (Attiva esclusioni dalla scansione).***
    - ***Scan Exclusion (Esclusioni dalla scansione) > Apply scan exclusion settings to all scan types (Applica impostazioni di esclusione dalla scansione a tutti i tipi di scansione).***
    - ***Scan Exclusion List (Directories) (Elenco esclusioni dalla scansione (directory)) > Exclude directories where Trend Micro products are installed (Escludi directory in cui sono installati i prodotti Trend Micro).***
    - Accertarsi che i percorsi delle cartelle ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** e ***G:*** siano presenti in Exclusion List (Elenco esclusioni).

25. Fare clic sulla scheda ***Action (Azione)***.

26. Lasciare le impostazioni predefinite e deselezionare le seguenti opzioni:

    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected (Visualizza un messaggio di notifica sugli endpoint al rilevamento di virus/malware).***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected (Visualizza un messaggio di notifica sugli endpoint al rilevamento di spyware/grayware).***

27. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.

28. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Scheduled Scan Settings (Impostazioni per la scansione programmata)***.

29. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.

30. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
31. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Scan Settings (Impostazioni scansione) > Scan Now Settings (Impostazioni per la scansione immediata)***. Viene visualizzata la schermata ***Scan Now Settings (Impostazioni per la scansione immediata)***.
32. Fare clic sulla scheda ***Target (Destinazione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
    - ***Scan Now Settings (Impostazioni per la scansione immediata) > Enable virus/malware scan (Attiva scansione virus/malware).***
    - ***Scan Now Settings (Impostazioni per la scansione immediata) > Enable spyware/grayware scan (Attiva scansione spyware/grayware).***
    - ***Files to Scan (File da analizzare) > File types scanned by IntelliScan (Tipi di file analizzati da IntelliScan).***
    - ***Scan Settings (Impostazioni scansione) > Scan compressed files (Analizza file compressi).***
    - ***Scan Settings (Impostazioni scansione) > Scan OLE objects (Analizza oggetti OLE).***
    - ***Virus/Malware Scan settings only (Solo impostazioni di scansione virus/malware) > Scan boot area (Analizza area di avvio).***
    - ***CPU Usage (Utilizzo CPU) > Low (Basso).***
33. Fare clic sulla scheda ***Scan Exclusion (Esclusione scansione)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:
    - ***Scan Exclusion (Esclusioni dalla scansione) > Enable scan exclusion (Attiva esclusioni dalla scansione).***
    - ***Scan Exclusion (Esclusioni dalla scansione) > Apply scan exclusion settings to all scan types (Applica impostazioni di esclusione dalla scansione a tutti i tipi di scansione).***
    - ***Scan Exclusion List (Directories) (Elenco esclusioni dalla scansione (directory)) > Exclude directories where Trend Micro products are installed (Escludi directory in cui sono installati i prodotti Trend Micro).***
    - Accertarsi che i percorsi delle cartelle ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:*** e ***G:*** siano presenti in Exclusion List (Elenco esclusioni).
34. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
35. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Scan now Settings (Impostazioni per la scansione immediata)***.
36. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.
37. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
38. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Web Reputation Settings (Impostazioni reputazione Web)***. Viene visualizzata la schermata ***Web Reputation Settings (Impostazioni reputazione Web)***.
39. Fare clic sulla scheda ***External Clients (Client esterni)*** e deselezionare ***Enable Web reputation policy on the following operating systems (Attiva criterio di reputazione Web sui seguenti sistemi operativi)***, se l'opzione era già selezionata durante l'installazione.

40. Fare clic sulla scheda ***Internal Agents (Agenti interni)*** e deselezionare ***Enable Web reputation policy on the following operating systems (Attiva criterio di reputazione Web sui seguenti sistemi operativi)***, se l'opzione era già selezionata durante l'installazione.
41. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
42. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Web Reputation (Reputazione Web)***.
43. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.
44. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
45. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Behavior Monitoring Settings (Impostazioni monitoraggio comportamento)***. Viene visualizzata la schermata ***Behavior Monitoring Settings (Impostazioni monitoraggio comportamento)***.
46. Deselezionare le opzioni ***Enable Malware Behavior Blocking (Attiva blocco comportamento malware)*** ed ***Enable Event Monitoring (Attiva monitoraggio eventi)***.
47. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
48. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Behavior Monitoring (Monitoraggio eventi)***.
49. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.
50. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
51. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Device Control Settings (Impostazioni di controllo dispositivi)***. Viene visualizzata la schermata ***Device Control Settings (Impostazioni di controllo dispositivi)***.
52. Fare clic sulla scheda ***External Agents (Agenti esterni)*** e deselezionare le seguenti opzioni:
    - ***Notification (Notifica) > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Visualizza un messaggio di notifica sugli endpoint quando OfficeScan rileva l'accesso di un dispositivo non autorizzato).***
    - ***Block the AutoRun function on USB storage devices (Blocca la funzione AutoRun sui dispositivi di memoria USB).***
    - ***Enable Device Control (Attiva controllo dispositivi).***
53. Fare clic sulla scheda ***Internal Agents (Agenti interni)*** e deselezionare le seguenti opzioni:
    - ***Notification (Notifica) > Display a notification message on endpoints when OfficeScan detects unauthorized device access (Visualizza un messaggio di notifica sugli endpoint quando OfficeScan rileva l'accesso di un dispositivo non autorizzato).***
    - ***Block the AutoRun function on USB storage devices (Blocca la funzione AutoRun sui dispositivi di memoria USB).***
    - ***Enable Device Control (Attiva controllo dispositivi).***
54. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
55. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Device Control Settings (Impostazioni di controllo dispositivi)***.

56. Dalle opzioni ***Settings (Impostazioni)***, selezionare nuovamente ***Device Control Settings (Impostazioni di controllo dispositivi)***. Viene visualizzata la schermata ***Device Control Settings (Impostazioni di controllo dispositivi)***.

57. Fare clic sulla scheda ***External Agents (Agenti esterni)*** e deselezionare ***Enable Device Control (Attiva controllo dispositivi)***.

58. Fare clic sulla scheda ***Internal Agents (Agenti interni)*** e deselezionare ***Enable Device Control (Attiva controllo dispositivi)***.

59. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.

60. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Device Control Settings (Impostazioni di controllo dispositivi)***.

61. Dal riquadro a sinistra, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.

62. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.

63. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Privileges and Other Settings (Privilegi e altre impostazioni)***.

64. Fare clic sulla scheda ***Privileges (Privilegi)*** e selezionare solo le seguenti opzioni, lasciando deselezionate le altre:

    - ***Scan Privileges (Privilegi scansione) > Configure Manual Scan Settings (Configura impostazioni per la scansione manuale).***
    - ***Scan Privileges (Privilegi scansione) > Configure Real-time Scan Settings (Configura impostazioni di scansione in tempo reale).***
    - ***Scan Privileges (Privilegi scansione) > Configure Scheduled Scan Settings (Configura impostazioni per la scansione programmata).***
    - ***Proxy Setting Privileges (Privilegi impostazione proxy) > Allow the agent user to configure proxy settings (Consenti all'utente dell'agente di configurare le impostazioni del proxy).***
    - ***Uninstallation (Disinstallazione) > Requires a password (Richiede una password).*** Inserire una password idonea e confermarla.
    - ***Unload and Unlock > Requires a password (Scarica e sblocca > Richiede una password).*** Inserire una password idonea e confermarla.

65. Fare clic sulla scheda ***Other Settings (Altre impostazioni)***.

66. Deselezionare tutte le opzioni.

NOTA: È importante deselezionare le opzioni seguenti.

- ***OfficeScan Agent Self-protection (Protezione automatica agente OfficeScan) > Protect OfficeScan agent services (Proteggi servizi agente OfficeScan).***
- ***OfficeScan Agent Self-protection (Protezione automatica agente OfficeScan) > Protect files in the OfficeScan agent installation folder (Proteggi i file nella cartella di installazione dell'agente OfficeScan).***
- ***OfficeScan Agent Self-protection (Protezione automatica agente OfficeScan) > Protect OfficeScan agent registry keys (Proteggi chiavi di registro agente OfficeScan).***
- ***OfficeScan Agent Self-protection (Protezione automatica agente OfficeScan) > Protect OfficeScan agent processes (Proteggi processi agente OfficeScan).***

67. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
68. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Privileges and Other Settings (Privilegi e altre impostazioni)***.
69. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Agent Management (Gestione agenti)***.
70. Sul lato sinistro, selezionare ***OfficeScan Server (Server OfficeScan)***.
71. Dalle opzioni ***Settings (Impostazioni)***, selezionare ***Additional Service Settings (Impostazioni servizi aggiuntivi)***.
72. Deselezionare l'opzione ***Enable service on the following operating systems (Attiva il servizio sui seguenti sistemi operativi)***.
73. Fare clic su ***Apply to All Agents (Applica a tutti gli agenti)***.
74. Fare clic su ***Close (Chiudi)*** per chiudere la schermata ***Additional Service Settings (Impostazioni servizi aggiuntivi)***.
75. Dal riquadro superiore, selezionare il collegamento ***Agents (Agenti) > Global Agent Settings (Impostazioni globali agenti)***.
76. Selezionare solo le seguenti opzioni, lasciando deselezionate le altre.
    - ***Scan Settings for Large Compressed Files (Impostazioni scansione per i file compressi di grandi dimensioni) > Do not scan files if the size exceeds 2 MB (Non analizzare i file di dimensioni superiori a 2 MB)***. Effettuare queste operazioni per ***Real-Time Scan (Scansione in tempo reale)*** e ***Manual Scan (Scansione manuale) / Schedule Scan (Scansione programmata) / Scan Now (Scansione immediata)***.
    - ***Scan Settings for Large Compressed Files (Impostazioni scansione per i file compressi di grandi dimensioni) > In a compressed file scan only the first 100 files (Analizza solo i primi 100 file di un file compresso).*** Effettuare queste operazioni per ***Real-Time Scan (Scansione in tempo reale)*** e ***Manual Scan (Scansione manuale) / Schedule Scan (Scansione programmata) / Scan Now (Scansione immediata)***.
    - ***Scan Settings (Impostazioni scansione) > Exclude the OfficeScan server database folder from Real-time Scan (Escludi la cartella del database del server OfficeScan dalla scansione in tempo reale).***
    - ***Scan Settings OfficeScan (Impostazioni scansione) > Exclude Microsoft Exchange server folders and files from scans (Escludi le cartelle e i file del server Microsoft Exchange dalle scansioni).***
77. Fare clic su ***Save (Salva)***.
78. Dal riquadro superiore, selezionare il collegamento ***Updates (Aggiornamenti) > Agents (Agenti) > Manual Updates (Aggiornamenti manuali)***.
79. Selezionare ***Manually select agents (Seleziona agenti manualmente)*** e fare clic su ***Select (Seleziona)***.
80. Fare doppio clic sul nome di dominio appropriato in ***OfficeScan Server (Server OfficeScan)***.
81. Selezionare il sistema client, uno alla volta, e fare clic su ***Initiate Update (Avvia aggiornamento)***.
82. Fare clic su ***OK*** nella finestra del messaggio.
83. Fare clic su ***Log off (Esci)*** e chiudere la console Web di OfficeScan.

Linee guida da seguire dopo l'installazione di Trend Micro OfficeScan

1. Attivare Loopback Connection (Connessione loopback). Per ulteriori informazioni, consultare Attivazione di Loopback Connection (Connessione loopback) a pagina 6.

2. Configurare il servizio Browser di computer. Per ulteriori informazioni, consultare Configurazione del servizio Browser di computer dopo l'installazione dell'antivirus a pagina 7.

Risoluzione dei problemi inerenti a domini o sistemi non elencati nella finestra Domains and Endpoints (Domini ed endpoint)

Durante il metodo di installazione push preferito per Trend Micro OfficeScan Client/Server Edition 11.0 SP1 e Trend Micro OfficeScan Client/Server Edition XG 12.0, i domini e i sistemi devono essere elencati per effettuare l'installazione nel sistema. La procedura seguente fornisce due opzioni per l'installazione del software antivirus sui client (acquisizione, revisione e INW).

Per 11.0 SP1, vedere Trend Micro OfficeScan - Procedura di distribuzione di una nuova installazione (metodo di installazione push preferito per 11.0 SP1) a pagina 59.
Per 12.0, vedere Trend Micro OfficeScan - Procedura di distribuzione di una nuova installazione (metodo di installazione push preferito per 12.0) a pagina 70.

1. Utilizzare gli indirizzi IP delle macchine client (acquisizione, revisione e INW) sulla console di gestione e procedere come segue:

    a. Inserire l'IP di ogni sistema client nella casella ***Search for endpoints (Cerca endpoint)***, uno alla volta, e premere ***Invio***.

    b. Indicare ***<nome dominio>\nome utente e password*** e fare clic su ***Log on (Accedi)***.

    c. Scegliere uno dei seguenti passaggi, a seconda della versione di Trend Micro:

        i. Per 11.0 SP1, tornare al passaggio 10 a pagina 59.

        ii. Per 12.0, tornare al passaggio 10 a pagina 71.

2. Se l'indirizzo IP dei sistemi è noto o se l'opzione precedente non funziona, accedere a ogni macchina client (acquisizione, revisione e server INW) e procedere come segue:

    a. Accedere come **Administrator (Amministratore)** o come membro di tale gruppo su tutte le macchine client.

    b. Fare clic su ***Start > Run (Esegui)***.

    c. Digitare ***<Anti-Virus Management Console_server_IP_address> (\\<indirizzo_IP_server_console_gestione_antivirus>)*** e premere ***Invio***. Quando viene chiesto, inserire nome utente e password dell'amministratore.

    d. Accedere a ***<Anti-Virus Management Console_server_IP _address>\ofsscan (\\<indirizzo_IP_server_console_gestione_antivirus>\ofsscan)*** e fare doppio clic su ***AutoPcc.exe***. Quando viene chiesto, inserire nome utente e password dell'amministratore.

    e. Al termine dell'installazione, riavviare i sistemi client.

f. Accedere come **Administrator (Amministratore)** o come membro di tale gruppo su tutte le macchine client e attendere che l'icona di Trend Micro OfficeScan nella barra delle applicazioni diventi blu.

g. Scegliere uno dei seguenti passaggi, a seconda della versione di Trend Micro:

   i. Per 11.0 SP1, vedere Configurazione della console del server di Trend Micro OfficeScan per 11.0 SP1 a pagina 60.

   ii. Per 12.0, vedere Configurazione della console del server di Trend Micro OfficeScan per 12.0 a pagina 71.