Mac-Lab/CardioLab Anti-Virus Installation Instructions (EN)

Mac-Lab/CardioLab Software Version 6.9.6

Introduction

Anti-virus software supports facilities in complying with privacy regulations, such as HIPAA.

Document Use

Use this document to install validated anti-virus software for the Mac-Lab/CardioLab v6.9.6 system.

Revision History

Revision	Date	Comments
A	16 February 2016	Initial public release.
B	9 June 2016	Trend Micro update to support CO_2.
C	16 May 2017	Updates to McAfee ePolicy Ochestrator, Trend Micro, and Symantec.
D	10 July 2017	Updates for Symantec 12.1.6 MP5, Trend Micro 11.0 SP1, McAfee ePO 5.9, and McAfee VSE 8.8 Patch 9.
E	14 August 2017	Remove references to McAfee ePolicy Orchestrator 5.9 and McAfee VirusScan Enterprise 8.8 Patch 9. Add 6.9.6 R3 UI languages.
F	25 September 2017	Add McAfee ePO 5.9 and McAfee VSE 8.8 Patch 9. Update links for Trend Micro 11 and 12.

Getting Started

Anti-Virus Requirements

⚠

WARNING: **ANTI-VIRUS SOFTWARE INSTALLATION REQUIRED**

The System is delivered without anti-virus protection. Ensure a validated anti-virus is installed on the system before connecting to any network. Lack of validated virus protection could lead to system instability or failure.

Note the following requirements:

- Anti-virus software is not provided with the Mac-Lab/CardioLab system and is the customer's responsibility to acquire, install, and maintain.
- The customer is responsible for updating anti-virus definition files.
- If a virus is found contact the facility System Administrator and GE Technical Support.
- Install only the anti-virus software packages listed in the listed in the Validated Anti-Virus Software section.
- Log in as an Administrator or member of that group to perform the activities in this document.
- Use a language version of the validated anti-virus software that matches the operating system language if possible. If there is no validated anti-virus software that matches the operating system language, install the English version of the anti-virus software.

Validated Anti-Virus Software

⚠

WARNING: **SYSTEM INSTABILITY**

Do not install or use unvalidated anti-virus software (including unvalidated versions). Doing so may result in system instability or failure. Use only validated anti-virus software in the appropriate language version.

NOTE: If the language specific anti-virus software is not available, install the English version of anti-virus software.

The Mac-Lab/CardioLab v6.9.6 systems have been validated to run with the software listed in the following table.

Supported Anti-Virus Software	Supported MLCL Languages	Supported Anti-Virus Software Version
McAfee VirusScan Enterprise	English, French, German, Italian, Spanish, Swedish, Norwegian, Danish, Dutch, Chinese, Japanese	8.8 Patch 3 8.8 Patch 4 8.8 Patch 8 8.8 Patch 9
McAfee ePolicy Orchestrator (with McAfee VirusScan Enterprise)	English, French, German, Italian, Spanish, Swedish, Norwegian, Danish, Dutch, Chinese, Japanese	v5.0 v5.3.2 v5.9

Supported Anti-Virus Software	Supported MLCL Languages	Supported Anti-Virus Software Version
Symantec EndPoint Protection	English, French, German, Italian, Spanish, Swedish, Norwegian, Danish, Dutch, Chinese, Japanese	12.1.2, 12.1.6 MP5, 14.0 MP1
Trend Micro OfficeScan Client/Server Edition	English, French, German, Italian, Spanish, Swedish, Norwegian, Danish, Dutch, Chinese, Japanese	10.6 SP2, 11.0 SP1, XG 12.0

The supported anti-virus software is available in the languages listed in the following table.

MLCL Version	Supported MLCL Languages
M6.9.6 R1	English
M6.9.6 R2	English, French, German
M6.9.6 R3	English, French, German, Italian, Spanish, Swedish, Norwegian, Danish, Dutch, Chinese, Japanese

Anti-virus Management Console Server Configuration

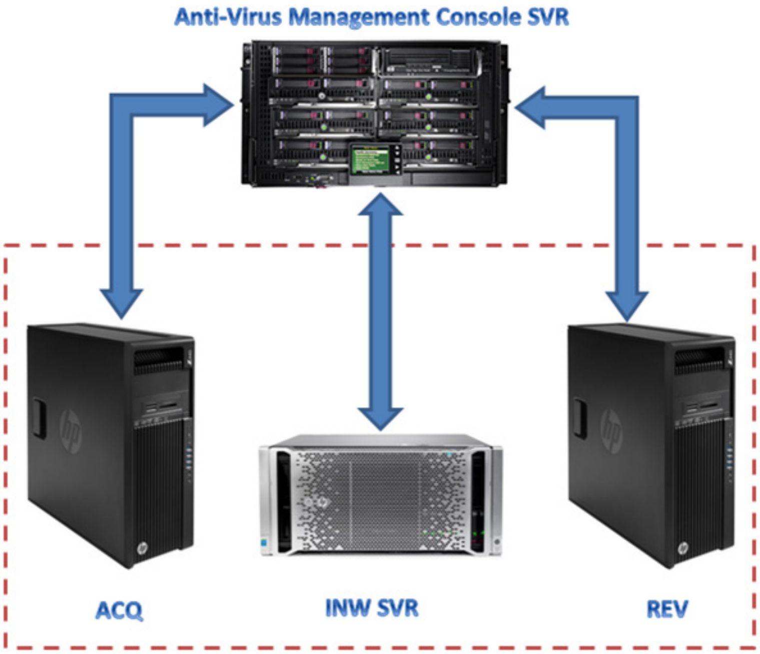
The anti-virus management console is required to be installed on the Anti-virus Management Console Server.

The communication between Anti-virus Management Console Server and Mac-Lab/CardioLab devices can be accomplished in different ways depending on the environment:

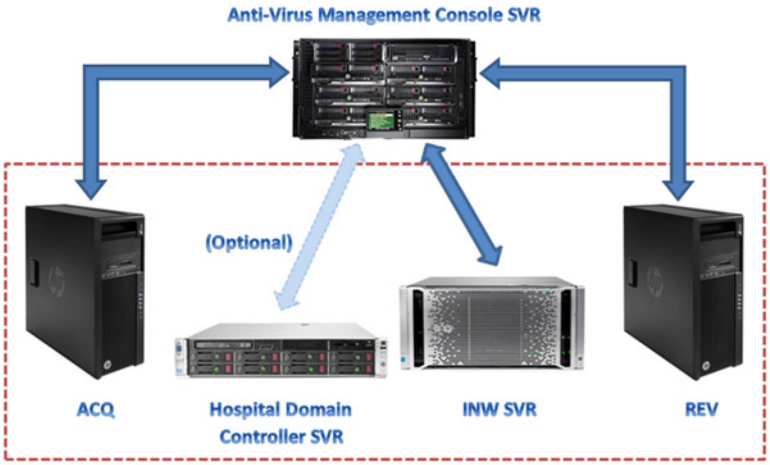
1. INW Domain Controller Environment - Anti-virus Management Console SVR not in INW Server Domain
   - Communication Type - 1 <Same network with same subnet mask>
   - Communication Type - 2 <Different network with different subnet mask>
2. Hospital Domain Controller Environment - Anti-virus Management Console SVR not in Hospital Domain Controller Domain
   - Communication Type - 1 <Different network with different subnet mask>
3. Hospital Domain Controller Environment - Anti-virus Management Console SVR in Hospital Domain Controller Domain
   - Communication Type - 1 <Same network with same subnet mask>

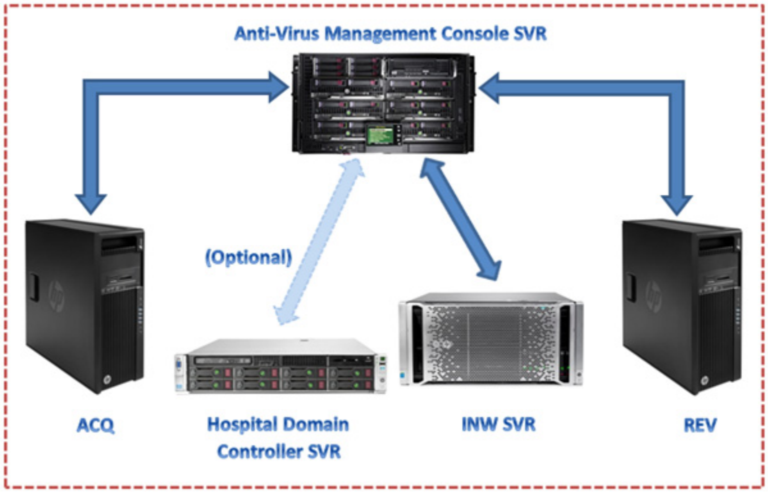
NOTE: The Anti-virus Management Console server should have two network ports. One network port to connect to the Centricity Cardiology INW network and the second network port to connect to the hospital network.

INW Domain Controller Environment Block Diagram


Anti-Virus Management Console SVR
ACQ
INW SVR
REV

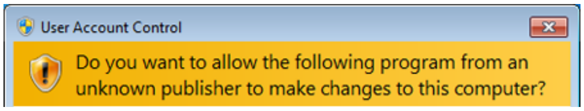
Hospital Domain Controller Environment Block Diagram


Anti-Virus Management Console SVR
(Optional)
ACQ
Hospital Domain Controller SVR
INW SVR
REV


Anti-Virus Management Console SVR
(Optional)
ACQ
Hospital Domain Controller SVR
INW SVR
REV

User Account Control

User Account Control is a Windows feature that prevents unauthorized changes to a computer. During certain procedures in this manual, a User Account Control message is displayed.


User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

When this message is displayed as a result of following the procedures in this manual, it is safe to continue.

Anti-Virus Installation Instructions

Click the anti-virus software you want to install:

- Symantec EndPoint Protection (12.1.2, 12.1.6 MP5, or 14.0 MP1) on page 7
- McAfee VirusScan Enterprise on page 14
- McAfee ePolicy Orchestrator on page 18
- Trend Micro OfficeScan Client/Server Edition 10.6 SP2 on page 37
- Trend Micro OfficeScan Client/Server Edition 11.0 SP1 on page 45
- Trend Micro OfficeScan Client/Server Edition XG 12.0 on page 54

Anti-Virus Software Common Installation Procedures

Use the procedures in this section when they are referenced in the anti-virus software installation instructions.

Disable Loopback Connection

On an Acquisition system connected to the Mac-Lab/CardioLab environment, disable the Loopback Connection to discover all client systems with the same subnet mask on the domain.

1. Log on as **Administrator** or a member of that group.
2. Right-click ***Network*** on the desktop and select ***Properties***.
3. Click ***Change adapter settings***.
4. Right-click ***Loopback Connection*** and select ***Disable***.
5. Restart the Acquisition system.

NOTE: Disabling the Loopback connection on the Acquisition system is required to discover all client systems with same subnet mask on the domain.

Enable Loopback Connection

On an Acquisition systems connected to the Mac-Lab/CardioLab environment, enable the Loopback Connection using the steps below.

1. Log on as **Administrator** or member of that group.
2. Right-click ***Network*** on the desktop and select ***Properties***.
3. Click ***Change adapter settings***.
4. Right-click ***Loopback Connection*** and select ***Enable***.
5. Restart the Acquisition system.

Configure Computer Browser Service Before Anti-Virus Installation

Check the Computer Browser service setting on networked Acquisition and Review systems to make sure it is configured correctly.

1. Click ***Start > Control Panel > Network and Sharing Center***.
2. Click ***Change advanced sharing settings***.
3. Expand ***Home or Work***.
4. Make sure ***Turn on file and printer sharing*** is selected.
5. Click ***Save changes***.
6. Click ***Start > Run***.
7. Type **services.msc** and press **Enter**.
8. Double-click the ***Computer Browser*** service.
9. Make sure the ***Startup type*** is set to ***Automatic***. If it's not set to Automatic, change it and click ***Start***.
10. Click ***OK***.
11. Close the ***Services*** window.

Configure Computer Browser Service After Anti-Virus Installation

After installing the anti-virus software, check the Computer Browser service setting on networked Acquisitions and Review systems to make sure it is configured correctly.

1. Click ***Start > Run***.
2. Type **services.msc** and press **Enter**.
3. Double-click the ***Computer Browser*** service.
4. Change the ***Startup type*** to ***Manual***.
5. Click ***OK***.
6. Close the ***Services*** window.

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

Installation Overview

Install Symantec EndPoint Protection in a networked Mac-Lab/CardioLab environment only. In a networked environment, the Symantec EndPoint Protection must be installed on the Anti-virus Management Console server and then deployed to the Centricity Cardiology INW server and Acquisition/Review workstation as clients. Use the following instructions to install and configure ***Symantec EndPoint Protection***.

Virus updates are the responsibility of the facility. Update the definitions regularly to ensure that the latest virus protection is on the system.

Pre-Installation Guidelines

1. The Symantec Anti-Virus Management Console is expected to be installed per Symentec instructions and working properly.
2. Log on as **Administrator** or a member of that group on all client systems (Acquisition, Review, and INW Server) to install the anti-virus software.
3. Open the command prompt in ***Run As Administrator*** mode.
4. Navigate to C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

NOTE: To configure the INW server, navigate to C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Type **UpdateRegSymantec.ps1** and press ***Enter***.
6. Confirm that the script executed successfully.

   If the above mentioned folder path is not present, perform the following steps for all MLCL systems, except the MLCL 6.9.6R1 INW server (Server OS: Windows Server 2008R2).

   a. Click ***Start*** button then ***Run***.

   b. Type **Regedit.exe** and click ***OK***.

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

   d. Locate and double-click the ***State*** registry.

   e. Change the ***Base*** to ***Decimal***.

   f. Change the ***Value data*** to ***146432***.

   g. Click ***OK*** and close the registry.
7. Disable the Loopback Connection. Refer to Disable Loopback Connection on page 6 for more information.
8. Configure the Computer Browser service. Refer to Configure Computer Browser Service Before Anti-Virus Installation on page 6 for more information.

Symantec EndPoint Protection - New Installation Deployment Steps (Preferred Push Installation Method)

1. Click ***Start > All Programs > Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager***.
2. Enter the user name and password to log in to Symantec Endpoint Protection Manager. (Click ***Yes*** if a security prompt displays.)
3. Check ***Do not show this Welcome Page again*** and click ***Close*** to close the welcome screen.

NOTE: For version 14.0 MP1, click ***Close*** to close the ***Getting Started on Symantec EndPoint Protection*** screen.

4. Click ***Admin*** in the ***Symantec EndPoint Protection Manager*** window.

5. Click ***Install Packages*** in the bottom pane.

6. Click ***Client Install Feature Set*** in the top pane.

7. Right click the ***Client Install Feature Set*** window and select ***Add***. The Add Client Install Feature Set window displays.

8. Enter the appropriate name and record it as it is needed later.

9. Make sure the ***Feature set version*** is ***12.1 RU2 and later***.

10. Select only the following features and unselect the other features.

    - ***Virus, Spyware, and Basic Download Protection***.
    - ***Advanced Download Protection***.

11. Click ***OK*** on the message box.

12. For versions 12.1.2 and 12.1.6 MP5 only, click ***OK*** to close the ***Add Client Install Feature Set*** window.

13. Click ***Home*** in the ***Symantec Endpoint Protection Manager*** window.

14. Depending on software version, do one of the following:

    - **Versions 12.1.2 and 12.1.6 MP5:** Select ***Install protection client to computers*** from the ***Common Tasks*** drop-down list in the top-right of the ***Home*** window. The Client Deployment Type screen displays.
    - **Version 14.0 MP1:** Click ***Clients*** in the ***Symantec Endpoint Protection Manager*** window. Click ***Install a client*** under ***Tasks***. The ***Client Deployment wizard*** screen displays.

15. Select ***New Package Deployment*** and click ***Next***.

16. Select the feature sets name created in step 8. Keep the other settings as default and click ***Next***.

NOTE: For version 14.1 MP1, under ***Scheduled Scans*** uncheck ***Delay scheduled scans when running on batteries and Allow user-defined scheduled scans to run when scan author is not logged on***.

17. Select ***Remote push*** and click ***Next***. Wait for the ***Computer selection*** screen to appear.

18. Expand ***<Domain>*** (example: INW). Systems connected to the domain are displayed in the ***Computer selection*** window.

NOTE: If all systems are not being recognized, click ***Search Network*** and click ***Find Computers***. Use the ***search by IP address*** detection method to identify the client systems (Acquisition, Review, and INW Server).

19. Select all Mac-Lab/CardioLab client machines connected to the domain and click **>>**. The ***Login Credentials*** screen displays.

20. Enter the user name, password and domain/computer name and click ***OK***.

21. Make sure all selected machines appear under ***Install Protection Client*** and click ***Next***.

22. Click ***Send*** and wait until the Symantec anti-virus software is deployed on all client systems (Acquisition, Review, and INW Server). When finished, the ***Deployment Summary*** screen displays.

23. Click ***Next*** and then click ***Finish*** to complete the Client Deployment Wizard.

24. Wait until the Symantec icon displays in system tray and then restart all the client machines (Acquisition, Review, and INW Server). Login with Administrator or as a member of that group on all client machines after the restart.

Symantec EndPoint Protection Server Console Configurations

1. Select ***Start > All Programs > Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager***. The Symantec EndPoint Protection Manager log on window opens.
2. Enter the Symantec Endpoint Protection Manager Console password and click ***Log On***.
3. Select the ***Policies*** tab and click ***Virus and Spyware Protection*** under ***Policies***. The ***Virus and Spyware Protection Policies*** window opens.
4. Click ***Add a Virus and Spyware Protection*** policy under ***Tasks***. The ***Virus and Spyware Protection*** window opens.
5. Under ***Windows Settings > Scheduled Scans***, click ***Administrator-Defined Scans***.
6. Select ***Daily Scheduled Scan*** and click ***Edit***. The ***Edit Scheduled Scan*** window opens.
7. Change scan name and description to ***Weekly Scheduled Scan*** and ***Weekly Scan at 00:00*** respectively.
8. Select ***Scan type*** as ***Full Scan***.
9. Select the ***Schedule*** tab.
10. Under ***Scanning Schedule***, select ***Weekly*** and change the time to ***00:00***.
11. Under ***Scan Duration*** uncheck ***Randomize scan start time within this period (recommended in VMs)*** and select ***Scan until finished (recommended to optimize scan performance)***.
12. Under ***Missed scheduled Scans*** uncheck ***Retry the scan within***.
13. Select the ***Notifications*** tab.
14. Uncheck ***Display a notification message on the infected computer*** and click ***OK***.
15. Select the ***Advanced*** tab in the ***Administrator-Defined Scans*** window.
16. Under ***Scheduled Scans*** uncheck ***Delay scheduled scans when running on batteries***, ***Allow user-defined scheduled scans to run when scan author is not logged on***, and ***Display notifications about detections when the user logs on***.

NOTE: For version 14.0 MP1, under ***Scheduled Scans*** uncheck ***Delay scheduled scans when running on batteries and Allow user-defined scheduled scans to run when scan author is not logged on***.

17. Under ***Startup and Triggered Scans*** uncheck ***Run an Active Scan when new definitions arrive***.

18. Under ***Windows Settings > Protection Technology***, click ***Auto-Protect***.
19. Select the ***Scan Details*** tab and select and lock ***Enable Auto-Protect***.
20. Select the ***Notifications*** tab and uncheck and lock ***Display a notification message on the infected computer*** and ***Display the Auto-Protect results dialog on the infected Computer***.
21. Select the ***Advanced*** tab and under ***Auto-Protect Reloading and Enablement***, lock the ***When Auto-Protect is disabled, Enable after:*** option.
22. Under ***Additional Options*** click ***File Cache***. The ***File Cache*** window opens.
23. Uncheck ***Rescan cache when new definitions load*** and click ***OK***.
24. Under ***Windows Settings > Protection Technology***, click ***Download Protection***.
25. Select the ***Notifications*** tab and uncheck and lock ***Display a notification message on the infected computer***.
26. Under ***Windows Settings > Protection Technology***, click ***SONAR***.
27. Select the ***SONAR Settings*** tab and uncheck and lock ***Enable SONAR***.
28. Under ***Windows Settings > Protection Technology***, click ***Early Launch Anti-Malware Driver***.
29. Uncheck and lock ***Enable Symantec early lauch anti-malware***.
30. Under ***Windows Settings > Email Scans***, click ***Internet Email Auto-Protect***.
31. Select the ***Scan Details*** tab and uncheck and lock ***Enable Internet Email Auto-Protect***.
32. Select the ***Notifications*** tab and uncheck and lock ***Display a notification message on the infected computer***, ***Display a progress indicator when email is being sent***, and ***Display a notification area icon***.
33. Under ***Windows Settings > Email Scans***, click ***Microsoft Outlook Auto-Protect***.
34. Select the ***Scan Details*** tab and uncheck and lock ***Enable Microsoft Outlook Auto-Protect***.
35. Select the ***Notifications*** tab and uncheck and lock ***Display a notification message on the infected computer***.
36. Under ***Windows Settings > Email Scans***, click ***Lotus Notes Auto-Protect***.
37. Select the ***Scan Details*** tab and uncheck and lock ***Enable Lotus Notes Auto-Protect***.
38. Select the ***Notifications*** tab and uncheck and lock ***Display a notification message on infected computer***.
39. Under ***Windows Settings > Advanced Options***, click ***Global Scan Options***.
40. Under ***Bloodhound(™) Detection Settings***, uncheck and lock ***Enable Bloodhound(™) heuristic virus detection***.
41. Under ***Windows Settings > Advanced Options***, click ***Quarantine***.
42. Select the ***General*** tab, under ***When New Virus Definitions Arrive***, select ***Do nothing***.
43. Under ***Windows Settings > Advanced Options***, click ***Miscellaneous***.

44. Select the ***Notifications*** tab and uncheck ***Display a notification message on the client computer when definitions are outdated***, ***Display a notification message on the client computer when Symantec Endpoint Protection is running without virus definitions*** and ***Display error messages with a URL to a solution***.

45. Click ***OK*** to close the ***Virus and Spyware Protection*** policy window.

46. Click ***Yes*** at the ***Assign Policies*** message box.

47. Select ***My Company*** and click ***Assign***.

48. Click ***Yes*** at the message box.

49. Under ***Policies*** click ***Firewall***.

50. Click ***Firewall policy*** under ***Firewall Policies*** and click ***Edit the policy*** under ***Tasks***.

51. Select the ***Policy Name*** tab and uncheck ***Enable this policy***.

52. Click ***OK***.

53. Under ***Policies*** click ***Intrusion Prevention***.

54. Click the ***Intrusion Prevention*** policy under ***Intrusion Prevention Policies*** and click ***Edit the policy*** under ***Tasks***.

55. Select the ***Policy Name*** tab and uncheck ***Enable this policy***.

56. Depending on software version, do one of the following:

    - **Version 12.1.2:** Click ***Settings*** from left pane.
    - **Versions 12.1.6 MP5 and 14.0 MP1:** Click ***Intrusion Prevention*** from left pane.

57. Uncheck and lock ***Enable Network Intrusion Prevention*** and ***Enable Browser Intrusion Prevention for Windows***.

58. Click ***OK***.

59. Under ***Policies*** click ***Application and Device Control***.

60. Click ***Application and Device Control Policy*** under ***Application and Device Control Policies*** and click ***Edit the policy*** under ***Tasks***.

61. Select the ***Policy Name*** tab and uncheck ***Enable this policy***.

62. Click ***OK***.

63. Under ***Policies*** click ***LiveUpdate***.

64. Select ***LiveUpdate Settings policy*** and under ***Tasks***, click ***Edit the policy***.

65. Under ***Overview > Windows Settings***, click ***Server Settings***.

66. Under ***Internal or External LiveUpdate Server***, ensure ***Use the default management server*** is selected and uncheck ***Use a LiveUpdate server***.

67. Click ***OK***.

68. Under ***Policies*** click ***Exceptions***.

69. Click ***Exceptions policy*** and under ***Tasks***, click ***Edit the policy***.

70. Depending on software version, do one of the following:

- **Versions 12.1.2 and 12.1.6 MP5:** Click ***Exceptions > Add > Windows Exceptions > Folder***.
- **Version 14.0 MP1:** Click the ***Add*** drop-down and select ***Windows Exceptions > Folder***.

71. Enter **C:\Program Files (x86)\GE Healthcare\MLCL**, **C:\Program Files\GE Healthcare\MLCL, D:\GEData\Studies**, **E:\**, **G:\** folder paths one at a time and perform the following:

    a. Ensure ***Include subfolders*** is selected.

NOTE: Click ***Yes*** if the ***Are you sure you want to exclude all subfolders from protection?*** message box displays.

    b. Select ***All*** from ***Specify the type of scan that excludes this folder***.

    c. For version 14.0 MP1, Click ***OK*** to add the exception.

72. Click ***OK***.

73. Click ***Assign the policy*** under ***Tasks***.

74. Select ***My Company*** and click ***Assign***.

75. Click ***Yes***.

76. Click ***Clients*** from left pane and select the ***Policies*** tab.

77. Under ***My Company*** select ***Default Group*** and uncheck ***Inherit policies and settings from parent group "My Company"*** and click ***Communications Settings*** under ***Location-Independent Policies and Settings***.

NOTE: If a warning message displays, click ***OK*** and click ***Communications Settings*** under ***Location-Independent Policies and Settings*** again.

78. Under ***Download***, make sure ***Download policies and content from the management server*** is checked and ***Push mode*** is selected.

79. Click ***OK***.

80. Click ***General Settings*** under ***Location-independent Policies and Settings***.

81. Select the ***Tamper Protection*** tab and uncheck and lock ***Protect Symantec security software from being tampered with or shut down***.

82. Click ***OK***.

83. Click ***Admin*** and select ***Servers***.

84. Under ***Servers***, select ***Local Site (My Site)***.

85. Under ***Tasks***, select ***Edit Site Properties***. The ***Site Properties for Locate Site (My Site)*** window opens.

86. Select ***LiveUpdate*** tab and under ***Download Schedule*** ensure the schedule is set to ***Every 4 hour(s)***.

87. Click ***OK***.

88. Click ***Log Off*** and close the Symantec EndPoint Protection Manager Console. Make sure Symantec Endpoint Protection Policies are pushed in client systems.

Symantec EndPoint Protection Post Installation Guidelines

1. Enable the Loopback Connection. Refer to Enable Loopback Connection on page 6 for more information.
2. Configure the Computer Browser service. Refer to Configure Computer Browser Service After Anti-Virus Installation on page 7 for more information.
3. Open the command prompt in ***Run As Administrator*** mode.
4. Navigate to C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

NOTE: To configure the INW server, navigate to C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec.

5. Type **RestoreRegSymantec.ps1** and press ***Enter***.
6. Confirm that the script executed successfully.
   Note: You must confirm that the **RestoreRegSymantec.ps1** script is executed successfully before continuing.

   If the above mentioned folder path is not present, perform the following steps for all MLCL systems, except the MLCL 6.9.6R1 INW server (Server OS: Windows Server 2008R2).

   a. Click ***Start*** button then ***Run***.

   b. Type **Regedit.exe** and click ***OK***.

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

   d. Locate and double-click the ***State*** registry.

   e. Change the ***Base*** to ***Decimal***.

   f. Change the ***Value data*** to ***65536***.

   g. Click ***OK*** and close the registry.

McAfee VirusScan Enterprise

Installation Overview

McAfee VirusScan Enterprise should be installed on an individual Mac-Lab/CardioLab system and it should be managed individually. Use the following instructions to install and configure McAfee VirusScan Enterprise.

Virus updates are the responsibility of the facility. Update the definitions regularly to ensure that the latest virus protection is on the system.

McAfee VirusScan Enterprise Installation Procedure

1. Log on as **Administrator** or as a member of that group.

2. Insert either the **McAfee VirusScan Enterprise 8.8 Patch 3**, **McAfee VirusScan Enterprise 8.8 Patch 4**, **McAfee VirusScan Enterprise 8.8 Patch 8 CD**, or **McAfee VirusScan Enterprise 8.8 Patch 9 CD** into the CD drive.
3. Double-click ***SetupVSE.Exe***. The Windows Defender dialog displays.
4. Click ***Yes***. The McAfee VirusScan Enterprise Setup screen displays.
5. Click ***Next***. The McAfee End User License Agreement screen displays.
6. Read the license agreement and complete any necessary fields, click ***OK*** when finished. The Select Setup Type screen displays.
7. Select ***Typical*** and click ***Next***. The Select Access Protection Level screen displays.
8. Select ***Standard Protection*** and click ***Next***. The Ready to Install screen displays.
9. Click ***Install*** and wait for the installation to complete. After successful installation of McAfee VirusScan Enterprise, the ***McAfee Virus Scan Enterprise Setup has completed successfully*** screen displays.
10. Uncheck the ***Run On-Demand Scan*** checkbox and click ***Finish***.
11. If the ***Update in Progress*** window displays, click ***Cancel***.
12. If a message box to restart the system displays, click ***OK***.
13. Restart the system.
14. Log on as **Administrator** or as a member of that group.

McAfee VirusScan Enterprise Configuration

1. Click ***Start > All Programs > McAfee > VirusScan Console***. The ***VirusScan Console*** screen appears.
2. Right click ***Access Protection*** and select ***Properties***. The ***Access Protection*** Properties screen appears.
3. Click the ***Access Protection*** tab and uncheck ***Enable access protection*** and ***Prevent McAfee services from being stopped***.
4. Click ***OK***.
5. Right click ***Buffer Overflow Protection*** and select ***Properties***. The ***Buffer Overflow Protection Properties*** screen appears.
6. Click the ***Buffer Overflow Protection*** tab and uncheck ***Show the messages dialog box when a buffer overflow is detected under Buffer overflow settings***.
7. Uncheck ***Enable buffer overflow protection*** under ***Buffer overflow settings***.
8. Click ***OK***.
9. Right click ***On-Delivery Email Scanner*** and select ***Properties***. The ***On-Delivery Email Scanner Properties*** screen appear.
10. Click the ***Scan items*** tab and uncheck following options under ***Heuristics***:
    - ***Find unknown program threats and trojans***.

- ***Find unknown macro threats***.
- ***Find attachments with multiple extensions***.

11. Uncheck ***Detect unwanted programs*** under ***Unwanted programs detection***.
12. Select ***Disabled*** for ***Sensitivity level*** under ***Artemis (Heuristic network check for suspicious files)***.
13. Click ***OK***.
14. Right click ***On-Delivery Email Scanner*** and select ***Disable***.
15. Right click ***On-Access Scanner*** and select ***Properties***. The ***On-Access Scan Properties*** screen appears.
16. Click the ***General*** tab and select ***Disabled*** for ***Sensitivity level*** under ***Artemis (Heuristic network check for suspicious files)***.
17. Click the ***ScriptScan*** tab and uncheck ***Enable scanning of scripts***.
18. Click the ***Blocking*** tab and uncheck ***Block the connection when a threat is detected in a shared folder***.
19. Click the ***Messages*** tab and uncheck ***Show the messages dialog box when a threat is detected and display the specified text in the message***.
20. Click ***All Processes*** from the left side pane.
21. Click the ***Scan Items*** tab and uncheck following options under Heuristics.
    - ***Find unknown unwanted programs and trojans***.
    - ***Find unknown macro threats***.
22. Uncheck ***Detect unwanted programs*** under ***Unwanted programs detection***.
23. Click the ***Exclusions*** tab and click ***Exclusions***. The ***Set Exclusions*** screen appears.
24. Click ***Add***. The ***Add Exclusion Item*** screen appears.
25. Select ***By name/location*** and click ***Browse***. The ***Browse for Files or Folders*** screen appears.
26. Navigate to ***C:\Program Files\GE Healthcare\MLCL\***, ***D:\GEData\Studies\***, ***E:\***, ***G:\*** folders one at a time and select ***OK***.
27. Select ***Also exclude subfolders*** in the ***Add Exclusion Item*** window and click ***OK***.
28. Make sure C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies\, E:\, G:\ folders are present in Set Exclusions window.
29. Click ***OK***.
30. Right click ***AutoUpdate*** and select ***Properties***. The McAfee AutoUpdate Properties - AutoUpdate screen appears.
31. Uncheck following options under ***Update Options***:
    - ***Get new detection engine and dats if available***.
    - ***Get other available updates (service packs, upgrades, etc.)***.
32. Click ***Schedule***. The Schedule Settings screen appears.
33. Uncheck ***Enable (scheduled task runs at specified time)*** under ***Schedule Settings***.

34. Click ***OK***.

35. Click ***OK***.

36. Right click the ***VirusScan Console*** window and select ***New On-Demand Scan Task***.

37. Rename the New Scan as ***Weekly Scheduled Scan***. The ***On-Demand Scan Properties - Weekly Scheduled Scan*** screen appears.

38. Click the ***Scan Items*** tab and uncheck ***Detect unwanted programs*** under ***Options***.

39. Uncheck following options under ***Heuristics***:

    - ***Find unknown programs threats***.
    - ***Find unknown macro threats***.

40. Click the ***Exclusions*** tab and click ***Exclusions***. The ***Set Exclusions*** screen appears.

41. Click ***Add***. The ***Add Exclusion Item*** screen appears.

42. Select ***By name/location*** and click ***Browse***. The ***Browse for Files or Folders*** screen appears.

43. Navigate to ***C:\Program Files\GE Healthcare\MLCL\***, ***D:\GEData\Studies\***, ***E:\***, ***G:\*** folders one at a time and select ***OK***.

44. Select ***Also exclude subfolders*** in the ***Add Exclusion Item*** window and click ***OK***.

45. Make sure ***C:\Program Files\GE Healthcare\MLCL\***, ***D:\GEData\Studies\***, ***E:\***, ***G:\*** folders are present in the ***Set Exclusions*** window.

46. Click ***OK***.

47. Click the ***Performance*** tab and select ***Disabled*** for ***Sensitivity level*** under ***Artemis (Heuristic network check for suspicious files)***.

48. Click ***Schedule***. The ***Schedule Settings*** screen appears.

49. Click the ***Task*** tab and select ***Enable (scheduled task runs at specified time)*** under ***Schedule Settings***.

50. Click the ***Schedule*** tab and select the following:

    a. Run task: Weekly.

    b. Start Time: 12:00 AM

    c. Every: 1 Weeks, Sunday.

51. Click ***OK***.

52. Click ***OK***.

53. Click ***Tools > Alerts*** in the ***VirusScan Console*** window. The Alert Properties screen appears.

54. Uncheck the ***On-Access Scan***, ***On-Demand Scan and scheduled scans***, ***Email Scan*** and ***AutoUpdate*** check boxes.

55. Click ***Destination***. The ***Alert Manager Client Configuration*** screen appears.

56. Select the ***Disable alerting*** check box.

57. Click ***OK***. The ***Alert Properties*** screen appears.

58. Select the ***Additional Alerting Options*** tab.

59. Select the ***Suppress all alerts (severities 0 to 4)*** option from the ***Severity Filter*** drop-down.

60. Select the ***Alert Manager Alerts*** tab.

61. Uncheck the ***Access Protection*** check box.

62. Click ***OK*** to close the ***Alert Properties*** window.

63. Close the ***VirusScan Console*** window.

McAfee ePolicy Orchestrator

Installation Overview

Install McAfee ePolicy Orchestrator on a networked Mac-Lab/CardioLab environment only. McAfee ePolicy Orchestrator must be installed on a Anti-virus Management Console server and McAfee VirusScan Enterprise should be deployed to the Centricity Cardiology INW server and Acquisition/Review workstations as a client. Use the following instructions to install and configure McAfee ePolicy Orchestrator.

The instructions below for pushing and configuring the McAfee VirusScan Enterprise supports Patch 3, Patch 4, Patch 8, and Patch 9.

Virus updates are the responsibility of the facility. Update the definitions regularly to ensure that the latest virus protection is on the system.

Pre-Installation Guidelines

1. The McAfee Anti-Virus Management Console is expected to be installed per McAfee instructions and working properly.

2. Log on as **Administrator** or a member of that group on all client systems (Acquisition, Review, and INW Server) to install the anti-virus software.

3. Disable the Loopback Connection. Refer to Disable Loopback Connection on page 6 for more information.

4. For deploying McAfee VirusScan Enterprise 8.8 Patch 9 contact McAfee to install UTN-USERFirst-Object and VeriSign Universal Root Certificates on INW Servers only. Restart the system once the certificates are installed.

NOTE: If UTN-USERFirst-Object and VeriSign Universal Root Certificates are not install the McAfee VirusScan Enterprise 8.8 Patch 9 installation fails on INW Servers.

5. For New Installation, add the following agent version to the McAfee ePolicy Orchestrator master repository in McAfee ePolicy Orchestrator Console: ***- McAfee Agent v5.0.5.658***

6. For New Installation, add the following package to the McAfee ePolicy Orchestrator master repository 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).

NOTE: VSE880LMLRP3.zip contains Patch 2 and Patch 3 installation packages. Patch 2 is for Windows 7 and Windows Server 2008 OS platform and Patch 3 is for Windows 8 and Windows Server 2012 OS platform. The McAfee installer installs the correct patch by identifying the Windows operating system version.

7. For New Installation, add the following extensions to the McAfee ePolicy Orchestrator extensions table in McAfee ePolicy Orchestrator Console:

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

NOTE: The VIRUSSCAN8800(348).zip and VIRUSSCANREPORTS120(228).zip can be found in McAfee VirusScan Enterprise 8.8 Patch 3 package.

The VIRUSSCAN8800(368).zip and VIRUSSCANREPORTS120(236).zip can be found in McAfee VirusScan Enterprise 8.8 Patch 4 package.

The VIRUSSCAN8800(511).zip and VIRUSSCANREPORTS120(311).zip can be found in McAfee VirusScan Enterprise 8.8 Patch 8 package.

The VIRUSSCAN8800(548).zip and VIRUSSCANREPORTS120(346).zip can be found in McAfee VirusScan Enterprise 8.8 Patch 9 package.

McAfee ePolicy Orchestrator 5.0 or 5.3.2 - New Installation Deployment Steps (Preferred Push Installation Method)

1. Depending on the software version, select ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** or ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console*** to log on to the ePolicy Orchestrator console.

NOTE: Click ***Continue with this website*** if the ***Security Alert*** message box displays.

2. Enter the username and password and click ***Log On***.
3. Select ***Menu > System > System Tree***. The System Tree window opens.
4. Click ***My Organization*** and with the focus on ***My Organization*** click ***System Tree Actions > New Systems*** from the bottom left corner of the screen.
5. Select ***Push agents and add systems to the current group (My Organization)*** and click ***Browse*** on Target systems.
6. Enter the **domain/local administrator** username and password and click ***OK***.
7. Select the ***INW*** domain from the ***Domain*** drop-down list.
8. Select the client machines (Acquisition, Review, and INW Server) connected to the domain and click ***OK***.

NOTE: If the domain name is not listed in the ***Domain*** drop-down, do the following:

- In the ***Browse for Systems*** windows, click ***Cancel***.
- In the ***New Systems*** window, enter the client machines (Acquisition, Review and INW server) system name manually in ***Target systems*** field and continue with the below steps.

9. Select ***Agent Version*** as M***cAfee Agent for Windows 4.8.0 (Current)*** or ***McAfee Agent for Windows 5.0.4 (Current)***. Enter the **domain administrator** username and password and click ***OK***.

10. In client machines (Acquisition, Review, and INW Server), confirm the directories are created correctly, depending on the patch version:

    - For patches 3 and 4 verify that ***C:\Program Files\McAfee\Common Framework*** directory is present and McAfee Agent is installed in the same directory.

NOTE: For the INW Server make sure the ***C:\Program Files (x86)\McAfee\Common Framework*** directory is present and McAfee Agent is installed in the same directory.

- For patch 8 verify that ***C:\Program Files\McAfee\Agent*** directory is present and McAfee Agent is installed in the same directory.

NOTE: For the INW Server make sure the ***C:\Program Files (x86)\McAfee\Common Framework*** directory is present.

11. Restart the client machines (Acquisition, Review, and INW Server) and log on as **domain administrator** or member of that group.

12. Depending on the software version, click ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** or ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console***.

13. Enter the username and password and click ***Log On***.

14. Click ***Menu > Systems > System Tree***.

15. Click ***My Organization*** and with the focus on ***My Organization*** click the ***Assigned Client Tasks*** tab.

16. Click ***Actions > New Client Task Assignment*** button at the bottom of the screen. The Client Task Assignment Builder screen displays.

17. Select the following:

    a. **Product:** McAfee Agent

    b. **Task Type:** Product Deployment

    c. **Task name:** Create New Task

18. On the ***Client Task Catalog: New Task- McAfee Agent: Product Deployment*** screen, complete the fields as follows:

    a. **Task Name:** Enter the appropriate task name

    b. **Target platforms:** Windows

    c. **Products and components:** VirusScan Enterprise version which is qualified for v6.9.6

    d. **Options:** Run at every policy enforcement (Windows only) if ***Options*** is available

19. Click ***Save***.
20. In the ***1 Select Task*** screen, select the following:
    a. **Product:** McAfee Agent
    b. **Task Type:** Product Deployment
    c. **Task Name:** Newly created task name
21. Click ***Next***. The 2 Schedule screen displays.
22. Select R***un immediately*** from ***Schedule type*** drop-down list.
23. Click ***Next***. The 3 Summary screen displays.
24. Click ***Save***. The ***System Tree*** screen displays.
25. Select the ***Systems*** tab and then select all the client machines (Acquisition, Review, and INW Server) which are connected to the domain.
26. Click ***Wake up Agents*** at bottom of the window.
27. Keep default settings and click ***OK***.
28. Wait until the McAfee icon displays in the system tray and then restart all the client machines (Acquisition, Review, and INW Server) and log in with **Administrator** or a member of that group on all client machines.
29. Click the ***Log Off*** link to close the McAfee ePolicy Orchestrator Console.

McAfee ePolicy Orchestrator 5.9.0 - New Installation Deployment Steps (Preferred Push Installation Method)

1. Click ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** to log on to the ePolicy Orchestrator console.

NOTE: Click ***Continue with this website*** if the ***Security Alert*** message box displays.

2. Enter the username and password and click ***Log On***.
3. Select ***Menu > System > System Tree***. The ***System Tree*** window opens.
4. Click ***My Organization*** and with the focus on ***My Organization*** click ***New Systems*** from the top of the screen.
5. Select ***Push agents and add systems to the current group (My Organization)*** and click ***Browse*** on Target systems.
6. Enter the **domain/local administrator** username and password and click ***OK***.
7. Select the ***INW*** domain from the ***Domain*** drop-down list.
8. Select the client machines (Acquisition, Review, and INW Server) connected to the domain and click ***OK***.

NOTE: If the domain name is not listed in the ***Domain*** drop-down, do the following:

- In the ***Browse for Systems*** windows, click ***Cancel***.
- In the ***New Systems*** window, enter the client machines (Acquisition, Review, and INW server) system name manually separated by a comma in ***Target systems*** field and continue with the below steps.

9. Select ***Agent Version*** as M***cAfee Agent for Windows 5.0.5 (Current)***. Enter the **domain administrator** username and password and click ***OK***.
10. In client machines (Acquisition, Review, and INW Server), confirm the ***C:\Program Files\McAfee\Agent*** directories are created correctly.
11. Restart the client machines (Acquisition, Review, and INW Server) and log on as **domain administrator** or member of that group.
12. Click ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** to log on to the ePolicy Orchestrator console.
13. Enter the username and password and click ***Log On***.
14. Click ***Menu > Systems > System Tree***.
15. Click ***My Organization*** and with the focus on ***My Organization*** click the ***Assigned Client Tasks*** tab.
16. Click ***Actions > New Client Task Assignment*** button at the bottom of the screen. The ***Client Task Assignment Builder*** screen displays.
17. Select the following:
    a. **Product:** McAfee Agent
    b. **Task Type:** Product Deployment
18. Click ***Task Actions > Create New Task***. The ***Create New Task*** screen displays.
19. On the ***Create New Task*** screen, complete the fields as follows:
    a. **Task Name:** Enter the appropriate task name
    b. **Target platforms:** Windows (uncheck all other options)
    c. **Products and components:** VirusScan Enterprise 8.8.0.1804
20. Click ***Save***. The ***Client Task Assignment Builde***r screen appears.
21. In the ***Client Task Assignment Builder*** screen, select the following:
    a. **Product:** McAfee Agent
    b. **Task Type:** Product Deployment
    c. **Task Name:** Newly created task name
    d. **Schedule Type:** Run immediately
22. Click ***Save***. The ***Assigned Client Tasks*** screen appears.
23. Select the ***Systems*** tab and then select all the client machines (Acquisition, Review, and INW Server) which are connected to the domain.
24. Click ***Wake up Agents*** at the bottom of the window.

25. Keep default settings and click ***OK***.

26. Wait until the McAfee icon displays in the system tray and then restart all the client machines (Acquisition, Review, and INW Server) and log in with **Administrator** or a member of that group on all client machines.

27. Click the ***Log Off*** link to close the McAfee ePolicy Orchestrator Console.

McAfee ePolicy Orchestrator 5.0 and 5.3.2 Server Console Configuration

1. Depending on the software version, click ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*** or ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console***.

2. Enter the username and password and click ***Log On***.

3. Click ***Menu > Systems > System Tree***.

4. Click ***My Organization*** and with the focus on My Organization click the ***Assigned Client Tasks*** tab.

5. Click the ***Actions > New Client Task Assignment*** button at the bottom of the screen. The ***Client Task Assignment Builder*** screen appears.

6. Select the following:

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

   b. ***Task Type:*** On Demand Scan

   c. ***Task name:*** Create New Task

7. On the ***Client Task Catalog: New Task - VirusScan Enterprise 8.8.0: On Demand Scan*** screen, complete the fields as follows:

   a. ***Task Name:*** Weekly Scheduled Scan

   b. ***Description:*** Weekly Scheduled Scan

8. Click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

9. Uncheck ***Detect unwanted programs*** under ***Options***.

10. Uncheck following options under Heuristics:

    - ***Find unknown program threats.***
    - ***Find unknown macro threats.***

11. Click ***Exclusions*** tab. The ***Exclusions*** screen appears.

12. Click ***Add***. The ***Add/Edit Exclusion*** Item screen appears.

13. Select ***By pattern*** and enter **C:\Program Files\GE Healthcare\MLCL\**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies\**, **E:\**, **G:\** folders one at a time and select Also exclude subfolders. Click ***OK***.

14. Click ***Performance*** tab. The ***Performance*** screen appear.

15. Select ***Disabled*** from ***Artemis (Heuristic network check for suspicious files)***.
16. Click ***Save***.
17. In the ***1 Select Task*** screen, select the following:
    - ***Product:*** VirusScan Enterprise 8.8.0
    - ***Task Type:*** On Demand Scan
    - ***Task Name:*** Weekly Scheduled Scan
18. Click ***Next***. The ***2 Schedule*** screen appears.
19. Select ***Weekly*** from the ***Scheduled type*** drop-down list and select ***Sunday***.
20. Set ***Start time*** as ***12:00 AM*** and select ***Run Once at that time***.
21. Click ***Next***. The ***3 Summary*** screen appears.
22. Click ***Save***. The ***System Tree*** screen appears.
23. Select the ***Assigned Policies*** tab. The ***Assigned Policies*** screen appears.
24. From the ***Product*** drop-down list, select ***VirusScan Enterprise 8.8.0***.
25. Click ***My Default*** for ***On-Access General Policies***. The ***VirusScan Enterprise 8.8.0 > On-Access General Policies > My Default*** screen appears.
26. Select ***Workstation*** from the ***Settings for*** drop-down list and click the ***General*** tab. The ***General*** screen appears.
27. Select ***Disabled*** from ***Artemis (Heuristic network check for suspicious files)***.
28. Click ***ScriptScan*** tab. The ***Script Scan*** screen appears.
29. Uncheck ***Enable scanning of scripts***.
30. Click the ***Blocking*** tab. The ***Blocking*** screen appears.
31. Uncheck ***Block the connection when a threatened file is detected in a shared folder***.
32. Click the ***Messages*** tab. The ***Messages*** screen appears.
33. Uncheck the ***Show the messages dialog box when a threat is detected and display the specified text in the message***.
34. Select ***Server*** from the ***Settings for*** drop-down list and click the ***General*** tab. The ***General*** screen appear.
35. Select ***Disabled*** from ***Artemis (Heuristic network check for suspicious files)***.
36. Click the ***ScriptScan*** tab. The ***Script Sca***n screen appears.
37. Make sure ***Enable scanning of scripts*** is unchecked.
38. Click the ***Blocking*** tab. The ***Blocking*** screen appears.
39. Uncheck ***Block the connection when a threatened file is detected in a shared folder***.
40. Click the ***Messages*** tab. The ***Messages*** screen appears.
41. Uncheck ***Show the messages dialog box when a threat is detected and display the specified text in the message***.

42. Click ***Save***.

43. Click ***My Default*** for ***On-Access Default Processes Policies***. The ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** screen appears.

44. Select ***Workstation*** from the ***Settings for*** drop-down list.

45. Click ***Scan Items*** tab. The ***Scan Items*** screen appears.

46. Uncheck the following options under ***Heuristics***:

    - ***Find unknown unwanted programs and trojans.***
    - ***Find unknown macro threats.***

47. Uncheck ***Detect unwanted programs*** under ***Unwanted programs detection***.

48. Click the ***Exclusions*** tab. The ***Exclusions*** screen appears.

49. Click ***Add***. The ***Add/Edit Exclusion Item*** screen appears.

50. Select ***By pattern*** and enter **C:\Program Files\GE Healthcare\MLCL\**, **D:\GEData\Studies\**, **E:\**, **G:\** folders one at a time and select ***Also exclude subfolders***. Click ***OK***.

51. Select ***Server*** from the ***Settings for*** drop-down list and click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

52. Uncheck the following options under ***Heuristics***:

    - ***Find unknown unwanted programs and trojans.***
    - ***Find unknown macro threats.***

53. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.

54. Click the ***Exclusions*** tab. The ***Exclusions*** screen appears.

55. Click ***Add***. The ***Add/Edit Exclusion Item*** screen appears.

56. Select ***By pattern*** and enter **C:\Program Files (x86)\GE Healthcare\MLCL\**, **D:\GEData\Studies\** folders one at a time and select ***Also exclude subfolders***. Click ***OK***.

57. Click ***Save***.

58. Click ***My Default*** for ***On-Access Low-Risk Processes Policies***. The ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies > My Default*** screen appears.

59. Select ***Workstation*** from the ***Settings for*** drop-down list.

60. Click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

61. Uncheck the following options under ***Heuristics***:

    - ***Find unknown unwanted programs and trojans.***
    - ***Find unknown macro threats.***

62. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.

63. Click the ***Exclusions*** tab. The ***Exclusions*** screen appears.

64. Click ***Add***. The ***Add/Edit Exclusion*** Item screen appears.

65. Select ***By pattern*** and enter **C:\Program Files\GE Healthcare\MLCL\**, **D:\GEData\Studies\**, **E:\**, **G:\** folders one at a time and select ***Also exclude subfolders***. Click ***OK***.

66. Select ***Server*** from the ***Settings for*** drop-down list and click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

67. Uncheck the following options under ***Heuristics***:

    - ***Find unknown unwanted programs and trojans.***
    - ***Find unknown macro threats.***

68. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.

69. Click the ***Exclusions*** tab. The ***Exclusions*** screen appears.

70. Click ***Add***. The ***Add/Edit Exclusion*** Item screen appears.

71. Select ***By pattern*** and enter **C:\Program Files (x86)\GE Healthcare\MLCL\**, **D:\GEData\Studies\** folders one at a time and select ***Also exclude subfolders***. Click ***OK***.

72. Click ***Save***.

73. Click ***My Default*** for ***On-Access High-Risk Processes Policies***. The ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** screen appears.

74. Select ***Workstation*** from the ***Settings for*** drop-down list.

75. Click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

76. Uncheck the following options under ***Heuristics***:

    - ***Find unknown unwanted programs and trojans.***
    - ***Find unknown macro threats.***

77. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.

78. Click the ***Exclusions*** tab. The ***Exclusions*** screen appears.

79. Click ***Add***. The ***Add/Edit Exclusion*** Item screen appears.

80. Select ***By pattern*** and enter **C:\Program Files\GE Healthcare\MLCL\**, **D:\GEData\Studies\**, **E:\**, **G:\** folders one at a time and select ***Also exclude subfolders***. Click ***OK***.

81. Select ***Server*** from the ***Settings for*** drop-down list and click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

82. Uncheck the following options under ***Heuristics***:

    - ***Find unknown unwanted programs and trojans.***
    - ***Find unknown macro threats.***

83. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.

84. Click the ***Exclusions*** tab. The ***Exclusions*** screen appears.

85. Click ***Add***. The ***Add/Edit Exclusion*** Item screen appears.

86. Select By pattern and enter **C:\Program Files (x86)\GE Healthcare\MLCL\**, **D:\GEData\Studies\** folders one at a time and select ***Also exclude subfolders***. Click ***OK***.

87. Click ***Save***.

88. Click ***My Default*** for ***On Delivery Email Scan Policies***. The ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default*** screen appears.

89. Select ***Workstation*** from the ***Settings for*** drop-down list.

90. Click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

91. Uncheck the following options under ***Heuristics***.

    - ***Find unknown program threats and trojans.***
    - ***Find unknown macro threats.***
    - ***Find attachments with multiple extensions.***

92. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.

93. Select ***Disabled*** from ***Artemis (Heuristic network check for suspicious files)***.

94. Uncheck ***Enable on-delivery email scanning*** under ***Scanning of email***.

95. Select ***Server*** from the ***Settings for*** drop-down list.

96. Click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

97. Uncheck the following options under ***Heuristics***:

    - ***Find unknown program threats and trojans.***
    - ***Find unknown macro threats.***
    - ***Find attachments with multiple extensions.***

98. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.

99. Select ***Disabled*** from ***Artemis (Heuristic network check for suspicious files)***.

100. Uncheck ***Enable on-delivery email scanning*** under ***Scanning of email***.

101. Click ***Save***.

102. Click ***My Default*** for ***General Options Policies***. The ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** screen appears.

103. Select ***Workstation*** form the ***Settings for*** drop-down list.

104. Click the ***Display Options*** tab. The ***Display Options*** screen appears.

105. Select the following under ***Console options***:

    - ***Display managed tasks in the client console.***
    - ***Disable default AutoUpdate task schedule.***

106. Select ***Server*** form the ***Settings for*** drop-down list.

107. Click the ***Display Options*** tab. The ***Display Options*** screen appears.

108. Select the following under ***Console options***.

    - ***Display managed tasks in the client console.***
    - ***Disable default AutoUpdate task schedule.***

109. Click ***Save***.

110.Click ***My Default*** for ***Alert Policies***. The ***VirusScan Enterprise 8.8.0 > Alter Policies > My Default*** screen appears.

111.Select ***Workstation*** from the ***Settings for*** drop-down list.

112.Click the ***Alert Manager Alerts*** tab. The ***Alert Manager Alerts*** screen appears.

113.Uncheck ***On-Access Scan***, ***On-Demand Scan and scheduled scans***, ***Email Scan*** and ***AutoUpdate*** under ***Components that generate alerts***.

114.Select ***Disable alerting*** under ***Alert Manager*** options.

115.Uncheck ***Access Protection*** under ***Components that generate alerts***.

116.Click ***Additional Alerting Options***. The ***Additional Alerting Options*** screen appears.

117.From the ***Severity Filters*** drop-down menu, select ***Suppress all alerts (severities 0 to 4)***.

118.Select ***Server*** from the ***Settings for*** drop-down list and select the ***Alert Manager Alerts*** tab. The ***Alert Manager Alerts*** screen appear.

119.Uncheck ***On-Access Scan***, ***On-Demand Scan and scheduled scans***, ***Email Scan*** and ***AutoUpdate*** under ***Components that generate alerts***.

120.Check ***Disable alerting*** under ***Alert Manager*** options.

121.Uncheck ***Access Protection*** under ***Components that generate alerts***.

122.Click ***Additional Alerting Options***. The Additional Alerting Options screen appears.

123.From the ***Severity Filters*** drop-down menu, select ***Suppress all alerts (severities 0 to 4)***.

124.Click ***Save***.

125.Click ***My Default*** for ***Access Protection Policies***. The ***VirusScan Enterprise 8.8.0 > Access Protection Policies > My Default*** screen appears.

126.Select ***Workstation*** from the ***Settings for*** drop-down list.

127.Click the ***Access Protection*** tab. The ***Access Protection*** screen appears.

128.Uncheck the following options under ***Access protection settings***:

- ***Enable access protection.***
- ***Prevent McAfee services from being stopped.***

129.Select ***Server*** from the ***Settings for*** drop-down list.

130.Click the ***Access Protection*** tab. The ***Access Protection*** screen appears.

131.Uncheck the following options under ***Access protection settings***:

- ***Enable access protection.***
- ***Prevent McAfee services from being stopped.***

132.Click ***Save***.

133.Click ***My Default*** for ***Buffer Overflow Protection Policies***. The ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** screen appears.

134.Select ***Workstation*** from the ***Settings for*** drop-down list.

135.Click the ***Buffer Overflow Protection*** tab. The ***Buffer Overflow Protection*** screen appears.

136.Uncheck ***Show the message dialog box when a buffer overflow is detected*** under ***Client system warning***.

137.Uncheck ***Enable buffer overflow protection*** under ***Buffer overflow settings***.

138.Select ***Server*** from the ***Settings for*** drop-down list.

139.Click the ***Buffer Overflow Protection*** tab. The ***Buffer Overflow Protection*** screen appears.

140.Uncheck ***Show the message dialog box when a buffer overflow is detected*** under ***Client system warning***.

141.Uncheck ***Enable buffer overflow protection*** under ***Buffer overflow settings***.

142.Click ***Save***.

143.From the ***Product*** drop-down menu, select ***McAfee Agent***. The ***Policies*** window for McAfee Agent appears.

144.Click ***My Default*** for ***Repository***. The ***McAfee Agent > Repository > My Default*** screen appears.

145.Click the ***Proxy*** tab. The ***Proxy*** screen appears.

146.Select ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** under ***Proxy settings***.

147.Click ***Save***.

148.Click the ***Systems*** tab.

149.Select all the client systems (Acquisition, Review and Centricity Cardiology INW server) into which the configured policies are to be deployed.

150.Select ***Wake Up Agents***. The ***Wake Up Agent*** screen appears.

151.Click ***OK***.

152.Log off ePolicy Orchestrator.

McAfee ePolicy Orchestrator 5.9.0 Server Console Configuration

1. Depending on the software version, click ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console***.
2. Enter the username and password and click ***Log On***.
3. Click ***Menu > Systems > System Tree***.
4. Click ***My Organization*** and with the focus on My Organization click the ***Assigned Client Tasks*** tab.
5. Click the ***Actions > New Client Task Assignment*** button at the bottom of the screen. The ***Client Task Assignment Builder*** screen appears.
6. Select the following:

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

   b. ***Task Type:*** On Demand Scan

7. Click ***Create New Task*** under ***Task Actions***. The ***Create New Task*** screen appears.

8. On the ***Create New Task*** screen, complete the fields as follows:

   a. ***Task Name:*** Weekly Scheduled Scan

   b. ***Description:*** Weekly Scheduled Scan

9. Click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

10. Uncheck ***Detect unwanted programs*** under ***Options***.

11. Uncheck following options under Heuristics:

    - ***Find unknown program threats.***
    - ***Find unknown macro threats.***

12. Click ***Exclusions*** tab. The ***Exclusions*** screen appears.

13. Click ***Add***. The ***Add/Edit Exclusion*** Item screen appears.

14. Select ***By pattern*** and enter **C:\Program Files\GE Healthcare\MLCL\**, **C:\Program Files (x86)\GE Healthcare\MLCL\, D:\GEData\Studies\**, **E:\**, **G:\** folders one at a time and select Also exclude subfolders. Click ***OK***.

15. Click ***Performance*** tab. The ***Performance*** screen appears.

16. Select ***Disabled*** from ***Artemis (Heuristic network check for suspicious files)***.

17. Click ***Save***. The ***Client Task Assignment Builder*** screen appears.

18. In the ***Client Task Assignment Builder*** screen, select the following:

    - ***Product:*** VirusScan Enterprise 8.8.0
    - ***Task Type:*** On Demand Scan
    - ***Task Name:*** Weekly Scheduled Scan

19. Select ***Weekly*** from the ***Scheduled type*** drop-down list and select ***Sunday***.

20. Set ***Start time*** as ***12:00 AM*** and select ***Run Once at that time***.

21. Click ***Save***. The ***Assigned Client Tasks*** screen appears.

22. Select the ***Assigned Policies*** tab. The ***Assigned Policies*** screen appears.

23. From the ***Product*** drop-down list, select ***VirusScan Enterprise 8.8.0***.

24. Click ***My Default*** for ***On-Access General Policies***. The ***VirusScan Enterprise 8.8.0 > On-Access General Policies > My Default*** screen appears.

25. Select ***Workstation*** from the ***Settings for*** drop-down list and click the ***General*** tab. The ***General*** screen appears.

26. Select ***Disabled*** from ***Artemis (Heuristic network check for suspicious files)***.

27. Click ***ScriptScan*** tab. The ***Script Scan*** screen appears.

28. Uncheck ***Enable scanning of scripts***.

29. Click the ***Blocking*** tab. The ***Blocking*** screen appears.
30. Uncheck ***Block the connection when a threatened file is detected in a shared folder***.
31. Click the ***Messages*** tab. The ***Messages*** screen appears.
32. Uncheck the ***Show the messages dialog box when a threat is detected and display the specified text in the message***.
33. Select ***Server*** from the ***Settings for*** drop-down list and click the ***General*** tab. The ***General*** screen appears.
34. Select ***Disabled*** from ***Artemis (Heuristic network check for suspicious files)***.
35. Click the ***ScriptScan*** tab. The ***Script Sca***n screen appears.
36. Make sure ***Enable scanning of scripts*** is unchecked.
37. Click the ***Blocking*** tab. The ***Blocking*** screen appears.
38. Uncheck ***Block the connection when a threatened file is detected in a shared folder***.
39. Click the ***Messages*** tab. The ***Messages*** screen appears.
40. Uncheck ***Show the messages dialog box when a threat is detected and display the specified text in the message***.
41. Click ***Save***. The Assigned Policies screen appears.
42. Click ***My Default*** for ***On-Access Default Processes Policies***. The ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies > My Default*** screen appears.
43. Select ***Workstation*** from the ***Settings for*** drop-down list.
44. Click ***Scan Items*** tab. The ***Scan Items*** screen appears.
45. Uncheck the following options under ***Heuristics***:
    - ***Find unknown unwanted programs and trojans.***
    - ***Find unknown macro threats.***
46. Uncheck ***Detect unwanted programs*** under ***Unwanted programs detection***.
47. Click the ***Exclusions*** tab. The ***Exclusions*** screen appears.
48. Click ***Add***. The ***Add/Edit Exclusion Item*** screen appears.
49. Select ***By pattern*** and enter **C:\Program Files\GE Healthcare\MLCL\**, **D:\GEData\Studies\**, **E:\**, **G:\** folders one at a time and select ***Also exclude subfolders***. Click ***OK***.
50. Select ***Server*** from the ***Settings for*** drop-down list and click the ***Scan Items*** tab. The ***Scan Items*** screen appears.
51. Uncheck the following options under ***Heuristics***:
    - ***Find unknown unwanted programs and trojans.***
    - ***Find unknown macro threats.***
52. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.
53. Click the ***Exclusions*** tab. The ***Exclusions*** screen appears.

54. Click ***Add***. The ***Add/Edit Exclusion Item*** screen appears.

55. Select ***By pattern*** and enter **C:\Program Files (x86)\GE Healthcare\MLCL\**, **D:\GEData\Studies\** folders one at a time and select ***Also exclude subfolders***. Click ***OK***.

56. Click ***Save***. The ***Assigned Policies*** screen appears.

57. Click ***My Default*** for ***On-Access Low-Risk Processes Policies***. The ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies > My Default*** screen appears.

58. Select ***Workstation*** from the ***Settings for*** drop-down list.

59. Click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

60. Uncheck the following options under ***Heuristics***:

    - ***Find unknown unwanted programs and trojans.***
    - ***Find unknown macro threats.***

61. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.

62. Click the ***Exclusions*** tab. The ***Exclusions*** screen appears.

63. Click ***Add***. The ***Add/Edit Exclusion*** Item screen appears.

64. Select ***By pattern*** and enter **C:\Program Files\GE Healthcare\MLCL\**, **D:\GEData\Studies\**, **E:\**, **G:\** folders one at a time and select ***Also exclude subfolders***. Click ***OK***.

65. Select ***Server*** from the ***Settings for*** drop-down list and click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

66. Uncheck the following options under ***Heuristics***:

    - ***Find unknown unwanted programs and trojans.***
    - ***Find unknown macro threats.***

67. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.

68. Click the ***Exclusions*** tab. The ***Exclusions*** screen appears.

69. Click ***Add***. The ***Add/Edit Exclusion*** Item screen appears.

70. Select ***By pattern*** and enter **C:\Program Files (x86)\GE Healthcare\MLCL\**, **D:\GEData\Studies\** folders one at a time and select ***Also exclude subfolders***. Click ***OK***.

71. Click ***Save***. The ***Assigned Policies*** screen appears.

72. Click ***My Default*** for ***On-Access High-Risk Processes Policies***. The ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies > My Default*** screen appears.

73. Select ***Workstation*** from the ***Settings for*** drop-down list.

74. Click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

75. Uncheck the following options under ***Heuristics***:

    - ***Find unknown unwanted programs and trojans.***
    - ***Find unknown macro threats.***

76. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.

77. Click the ***Exclusions*** tab. The ***Exclusions*** screen appears.

78. Click ***Add***. The ***Add/Edit Exclusion*** Item screen appears.

79. Select ***By pattern*** and enter **C:\Program Files\GE Healthcare\MLCL\**, **D:\GEData\Studies\**, **E:\**, **G:\** folders one at a time and select ***Also exclude subfolders***. Click ***OK***.

80. Select ***Server*** from the ***Settings for*** drop-down list and click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

81. Uncheck the following options under ***Heuristics***:

    - ***Find unknown unwanted programs and trojans.***
    - ***Find unknown macro threats.***

82. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.

83. Click the ***Exclusions*** tab. The ***Exclusions*** screen appears.

84. Click ***Add***. The ***Add/Edit Exclusion*** Item screen appears.

85. Select By pattern and enter **C:\Program Files (x86)\GE Healthcare\MLCL\**, **D:\GEData\Studies\** folders one at a time and select ***Also exclude subfolders***. Click ***OK***.

86. Click ***Save***. The ***Assigned Policies*** screen appears.

87. Click ***My Default*** for ***On Delivery Email Scan Policies***. The ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies > My Default*** screen appears.

88. Select ***Workstation*** from the ***Settings for*** drop-down list.

89. Click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

90. Uncheck the following options under ***Heuristics***.

    - ***Find unknown program threats and trojans.***
    - ***Find unknown macro threats.***
    - ***Find attachments with multiple extensions.***

91. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.

92. Select ***Disabled*** from ***Artemis (Heuristic network check for suspicious files)***.

93. Uncheck ***Enable on-delivery email scanning*** under ***Scanning of email***.

94. Select ***Server*** from the ***Settings for*** drop-down list.

95. Click the ***Scan Items*** tab. The ***Scan Items*** screen appears.

96. Uncheck the following options under ***Heuristics***:

    - ***Find unknown program threats and trojans.***
    - ***Find unknown macro threats.***
    - ***Find attachments with multiple extensions.***

97. Uncheck the ***Detect unwanted programs*** under ***Unwanted programs detection***.

98. Select ***Disabled*** from ***Artemis (Heuristic network check for suspicious files)***.

99. Uncheck ***Enable on-delivery email scanning*** under ***Scanning of email***.

100.Click ***Save***. The ***Assigned Policies*** screen appears.

101.Click ***My Default*** for ***General Options Policies***. The ***VirusScan Enterprise 8.8.0 > General Options Policies > My Default*** screen appears.

102.Select ***Workstation*** form the ***Settings for*** drop-down list.

103.Click the ***Display Options*** tab. The ***Display Options*** screen appears.

104.Select the following under ***Console options***:

- ***Display managed tasks in the client console.***
- ***Disable default AutoUpdate task schedule.***

105.Select ***Server*** from the ***Settings for*** drop-down list.

106.Click the ***Display Options*** tab. The ***Display Options*** screen appears.

107.Select the following under ***Console options***.

- ***Display managed tasks in the client console.***
- ***Disable default AutoUpdate task schedule.***

108.Click ***Save***. The ***Assigned Policies*** screen appears.

109.Click ***My Default*** for ***Alert Policies***. The ***VirusScan Enterprise 8.8.0 > Alter Policies > My Default*** screen appears.

110.Select ***Workstation*** from the ***Settings for*** drop-down list.

111.Click the ***Alert Manager Alerts*** tab. The ***Alert Manager Alerts*** screen appears.

112.Uncheck ***On-Access Scan***, ***On-Demand Scan and scheduled scans***, ***Email Scan*** and ***AutoUpdate*** under ***Components that generate alerts***.

113.Select ***Disable alerting*** under ***Alert Manager*** options.

114.Uncheck ***Access Protection*** under ***Components that generate alerts***.

115.Click ***Additional Alerting Options***. The ***Additional Alerting Options*** screen appears.

116.From the ***Severity Filters*** drop-down menu, select ***Suppress all alerts (severities 0 to 4)***.

117.Select ***Server*** from the ***Settings for*** drop-down list and select the ***Alert Manager Alerts*** tab. The ***Alert Manager Alerts*** screen appears.

118.Uncheck ***On-Access Scan***, ***On-Demand Scan and scheduled scans***, ***Email Scan*** and ***AutoUpdate*** under ***Components that generate alerts***.

119.Check ***Disable alerting*** under ***Alert Manager*** options.

120.Uncheck ***Access Protection*** under ***Components that generate alerts***.

121.Click ***Additional Alerting Options***. The Additional Alerting Options screen appears.

122.From the ***Severity Filters*** drop-down menu, select ***Suppress all alerts (severities 0 to 4)***.

123.Click ***Save***. The ***Assigned Policies*** screen appears.

124.Click ***My Default*** for ***Access Protection Policies***. The ***VirusScan Enterprise 8.8.0 > Access Protection Policies > My Default*** screen appears.

125.Select ***Workstation*** from the ***Settings for*** drop-down list.

126.Click the ***Access Protection*** tab. The ***Access Protection*** screen appears.

127.Uncheck the following options under ***Access protection settings***:

- ***Enable access protection.***
- ***Prevent McAfee services from being stopped.***
- ***Enable Enhanced Self-Protection.***

128.Select ***Server*** from the ***Settings for*** drop-down list.

129.Click the ***Access Protection*** tab. The ***Access Protection*** screen appears.

130.Uncheck the following options under ***Access protection settings***:

- ***Enable access protection.***
- ***Prevent McAfee services from being stopped.***
- ***Enable Enhanced Self-Protection.***

131.Click ***Save***. The ***Assigned Policies*** screen appears.

132.Click ***My Default*** for ***Buffer Overflow Protection Policies***. The ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies > My Default*** screen appears.

133.Select ***Workstation*** from the ***Settings for*** drop-down list.

134.Click the ***Buffer Overflow Protection*** tab. The ***Buffer Overflow Protection*** screen appears.

135.Uncheck ***Show the message dialog box when a buffer overflow is detected*** under ***Client system warning***.

136.Uncheck ***Enable buffer overflow protection*** under ***Buffer overflow settings***.

137.Select ***Server*** from the ***Settings for*** drop-down list.

138.Click the ***Buffer Overflow Protection*** tab. The ***Buffer Overflow Protection*** screen appears.

139.Uncheck ***Show the message dialog box when a buffer overflow is detected*** under ***Client system warning***.

140.Uncheck ***Enable buffer overflow protection*** under ***Buffer overflow settings***.

141.Click ***Save***. The ***Assigned Policies*** screen appears.

142.From the ***Product*** drop-down menu, select ***McAfee Agent***. The ***Policies*** window for McAfee Agent appears.

143.Click ***My Default*** for ***Repository***. The ***McAfee Agent > Repository > My Default*** screen appears.

144.Click the ***Proxy*** tab. The ***Proxy*** screen appears.

145.Make sure ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)*** under ***Proxy settings*** is selected.

146.Click ***Save***. The ***Assigned Policies*** screen appears.

147.Click the ***Systems*** tab.

148.Select all the client systems (Acquisition, Review, and Centricity Cardiology INW server) into which the configured policies are to be deployed.

149.Select ***Wake Up Agents***. The ***Wake Up Agent*** screen appears.

150.Click ***OK***.

151.Log off ePolicy Orchestrator.

McAfee ePolicy Orchestrator Post Installation Guidelines

Enable the Loopback Connection. Refer to Enable Loopback Connection on page 6 for more information.

Trend Micro OfficeScan Client/Server Edition 10.6 SP2

Installation Overview

Install Trend Micro OfficeScan Client/Server Edition on a networked Mac-Lab/CardioLab environment only. Trend Micro OfficeScan must be installed on the Anti-virus Management Console server and then deployed to Centricity Cardiology INW server and Acquisition/Review workstation as clients. Use the following instructions to install ***Trend Micro OfficeScan Client/ Server Edition***.

Virus updates are the responsibility of the facility. Update the definitions regularly to ensure that the latest virus protection is on the system.

Pre-Installation Guidelines

1. The Trend Micro Anti-Virus Management Console is expected to be installed per Trend Micro instructions and working properly.
2. During installation of Trend Micro OfficeScan do the following on Anti-Virus Management Console server:
    a. Uncheck ***Enable firewall*** in the ***Anti-virus Feature*** window.

    b. Select ***No, Please do not enable assessment mode*** in the ***Anti-spyware Feature*** window.

    c. Uncheck ***Enable web reputation policy*** in the ***Web Reputation Feature*** window.
3. Trend Micro OfficeScan is not recommended when using the $\boldsymbol{CO_2}$ feature with PDM in Mac-Lab/CardioLab systems.
4. If Trend Micro OfficeScan is required:
    a. It is recommended to configure a separate Trend Micro Anti-Virus Management Console server for the Mac-Lab/CardioLab systems. A global change to the Anti-Virus settings is required in order to use the $\boldsymbol{CO_2}$ feature with PDM in Mac-Lab/CardioLab systems.

    b. If a separate Trend Micro Anti-Virus Management Console server cannot be configured, a change to global settings is required to the existing Trend Micro Anti-Virus Management Console server after the installation. This change will impact all client systems connected to the existing Trend Micro Anti-Virus Management Console server and should be reviewed with IT personnel before proceeding.
5. Log on as **Administrator** or a member of that group on all client systems (Acquisition, Review, and INW Server) to install the anti-virus software.
6. Disable the Loopback Connection. Refer to Disable Loopback Connection on page 6 for more information.
7. Configure the Computer Browser service. Refer to Configure Computer Browser Service Before Anti-Virus Installation on page 6 for more information.

Trend Micro OfficeScan - New Installation Deployment Steps (Preferred Push Installation Method)

1. Click ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console***.

NOTE: Continue by selecting ***Continue to this website (not recommended)***. In the Security Alert window, check ***In the future, do not show this warning*** and click ***OK***.

2. If you receive a certificate error indicating that the site is not trusted, manage your certificates to include Trend Micro OfficeScan.
3. If prompted, install the ***AtxEnc*** add-ons. The Security Warning screen displays.
4. Click ***Install***.
5. Enter the username and password and click ***Log On***.
6. If prompted, click ***Update Now*** to install new widgets. Wait until the new widgets are updated. The update is completed screen will appear.
7. Click ***OK***.
8. From the left side menu bar, click ***Networked Computers > Client Installation > Remote***.
9. If prompted, install the ***AtxConsole*** add-ons. The Security Warning screen displays.
10. Click ***Install***.
11. Double-click ***My Company*** in the ***Remote Installation*** window. All domains will be listed under ***My Company***.
12. Expand the domain (Example: INW) from the list. All systems connected to the domain appear.
13. If domains or systems are not listed in the ***Domain and Computers*** window, do the following on each of the client systems (Acquisition, Review, and INW Server):
    a. Log in as Administrator or a member of that group on all client machines.
    b. Click ***Start > Run***.
    c. Type ***\\<Anti-Virus Management Console_server_IP_address>*** and press ***Enter***. When prompted enter the administrator username and password.
    d. Navigate to ***\\<Anti-Virus Management Console_server_IP _address>\ofsscan*** and double-click ***AutoPcc.exe***. When prompted enter the administrator username and password.
    e. Restart the client systems when the installation is complete.
    f. Log in as **Administrator** or a member of that group on all client machines and wait until the Trend Micro OfficeScan icon in system tray changes to blue.
    g. Skip the remaining steps in this procedure and go to the Trend Micro OfficeScan Server Console Configuration procedure.
14. Select the client machines (Acquisition, Review, and INW Server) and click ***Add***.
15. Type the <domain name>\username and password and click ***Log on***.

16. Select the client machines (Acquisition, Review, and INW Server) one at a time from the ***Selected Computers*** pane and click ***Install***.

17. Click ***Yes*** at the confirmation box.

18. Click ***OK*** at the ***Number of clients to which notifications were sent*** message box.

19. Restart all the client machines (Acquisition, Review, and INW Server) and Log in as Administrator or a member of that group on all client machines and wait until the Trend Micro OfficeScan icon in system tray changes to blue with a green tick mark symbol.

20. Click the ***Log Off*** link to close the ***OfficeScan Web Console***.

Trend Micro OfficeScan Server Console Configuration

1. Select ***Start > All Programs > TrendMicro Office Scan server <servername> > Office Scan Web Console***. The ***Trend Micro OfficeScan Login*** screen appears.

2. Enter the user name and password and click ***Login***. The ***Summary*** screen appears.

3. From the left side pane, select the ***Networked Computers > Client Management*** link.

4. On the right side, select ***OfficeScan Server***.

5. From the ***Settings*** options, select ***Scan Settings > Manual Scan Settings***. The ***Manual Scan Settings*** screen appears.

6. Click the ***Target*** tab and select only the following options and uncheck the remaining options:

   - ***Files to Scan > File types scanned by IntelliScan.***
   - ***Scan Settings > Scan compressed files.***
   - ***Scan Settings > Scan OLE objects.***
   - ***Virus/Malware Scan Settings Only > Scan boot area.***
   - ***CPU Usage > Low.***
   - ***Scan Exclusion > Enable scan exclusion.***
   - ***Scan Exclusion > Apply scan exclusion settings to all scan types.***
   - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed and select Add path to client Computers Exclusion list.***
   - Enter the **C:\Program Files (x86)\GE Healthcare\MLCL\**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:\** and **G:\** folders one at a time click ***Add***.

7. Click ***Apply to All Clients***.

8. Click ***OK*** at the ***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?*** message.

9. Click ***Close*** to close the ***Manual Scan Settings*** screen.

10. From the left side pane, select the ***Networked Computers > Client Management*** link.

11. On the right side, select ***OfficeScan*** Server.

12. From the ***Settings*** options, select ***Scan Settings > Real-time Scan Settings***. The ***Real-time Scan Settings*** screen appears.

13. Click the ***Target*** tab and select only the following options and uncheck the remaining options:

- ***Real-Time Scan Settings > Enable virus/malware scan.***
- ***Real-Time Scan Settings > Enable spyware/grayware scan.***
- ***Files to Scan > File types scanned by IntelliScan.***
- ***Scan Settings > Scan compressed files.***
- ***Scan Settings > Scan OLE objects.***
- ***Virus/Malware Scan Settings Only > Enable IntelliTrap.***
- ***Scan Exclusion > Enable scan exclusion.***
- ***Scan Exclusion > Apply scan exclusion settings to all scan types.***
- ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed.***
- Make sure the ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:\*** and ***G:\*** folder paths are present in the ***Exclusion List***.

14. Click the ***Action*** tab.
15. Keep the default settings and uncheck the following options:
    - ***Virus/Malware > Display a notification message on the client computer when virus/ malware is detected.***
    - ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected.***
16. Click ***Apply to All Clients***.
17. Click ***Close*** to close the ***Real-time Scan Settings*** screen.
18. From the left side pane, select the ***Networked Computers > Client Management*** link.
19. On the right side, select ***OfficeScan Server***.
20. From the ***Settings*** options, select ***Scan Settings > Scheduled Scan Settings***. The ***Scheduled Scan Settings*** screen appears.
21. Click the ***Target*** tab and select only the following options and uncheck the remaining options:
    - ***Scheduled Scan Settings > Enable virus/malware scan.***
    - ***Scheduled Scan Settings > Enable spyware/grayware scan.***
    - ***Schedule > Weekly, every Sunday, Start time: 00:00 hh:mm.***
    - ***Files to Scan > File types scanned by IntelliScan.***
    - ***Scan Settings > Scan compressed files.***
    - ***Scan Settings > Scan OLE objects.***
    - ***Virus/Malware Scan Settings Only > Scan boot area.***
    - ***CPU Usage > Low.***
    - ***Scan Exclusion > Enable scan exclusion.***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types.***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed.***
    - Make sure the ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:\*** and ***G:\*** folder paths are present in the Exclusion List.
22. Click the ***Action*** tab.

23. Keep the default settings and uncheck the following options:
    - ***Virus/Malware > Display a notification message on the client computer when virus/ malware is detected.***
    - ***Spyware/Grayware > Display a notification message on the client computer when spyware/grayware is detected.***
24. Click ***Apply to All Clients***.
25. Click ***Close*** to close the ***Scheduled Scan Settings*** screen.
26. From the left side pane, select the ***Networked Computers > Client Management*** link.
27. On the right side, select ***OfficeScan Server***.
28. From the ***Settings*** options, select ***Scan Settings > Scan Now Settings***. The ***Scan Now Settings*** screen appears.
29. Click the ***Target*** tab and select only the following options and uncheck the remaining options:
    - ***Scan Now Settings > Enable virus/malware scan.***
    - ***Scan Now Settings > Enable spyware/grayware scan.***
    - ***Files to Scan > File types scanned by IntelliScan.***
    - ***Scan Settings > Scan compressed files.***
    - ***Scan Settings > Scan OLE objects.***
    - ***Virus/Malware Scan Settings Only > Scan boot area.***
    - ***CPU Usage > Low.***
    - ***Scan Exclusion > Enable scan exclusion.***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types.***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed.***
    - Make sure the ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:\*** and ***G:\***
30. Click ***Apply to All Clients***.
31. Click ***Close*** to close the ***Scan Now Settings*** screen.
32. From the left side pane, select the ***Networked Computers > Client Management*** link.
33. On the right side, select ***OfficeScan Server***.
34. From the ***Settings*** options, select ***Web Reputation Settings***. The ***Web Reputation Settings*** screen appears.
35. Click the ***External Clients*** tab and uncheck ***Enable Web reputation policy on the following operating systems***, if selected already during installation.
36. Click the ***Internal Clients*** tab and uncheck ***Enable Web reputation policy on the following operating systems***, if selected already during installation.
37. Click ***Apply to All Clients***.
38. Click ***Close*** to close the ***Web Reputation*** screen.
39. From the left side pane, select the ***Networked Computers > Client Management*** link.
40. On the right side, select ***OfficeScan Server***.

41. From the ***Settings*** options, select ***Behavior Monitoring Settings***. The ***Behavior Monitoring Settings*** screen appears.

42. Uncheck the ***Enable Malware Behavior Blocking*** and ***Enable Event Monitoring*** options.

43. Click ***Apply to All Clients***.

44. Click ***Close*** to close the ***Behavior Monitoring*** screen.

45. From the left side pane, select the ***Networked Computers > Client Management*** link.

46. On the right side, select ***OfficeScan Server***.

47. From the ***Settings*** options, select ***Device Control Settings***. The ***Device Control Settings*** screen appears.

48. Click the ***External Clients*** tab and uncheck the following options:

    - ***Notification > Display a notification message on the client computer when OfficeScan detects unauthorized device access.***
    - ***Block the AutoRun function on USB storage devices.***
    - ***Enable Device Control.***

49. Click the ***Internal Clients*** tab and uncheck the following options:

    - ***Notification > Display a notification message on the client computer when OfficeScan detects unauthorized device access.***
    - ***Block the AutoRun function on USB storage devices.***
    - ***Enable Device Control.***

50. Click ***Apply to All Clients***.

51. Click ***Close*** to close the ***Device Control Settings*** screen.

52. From the left side pane, select the ***Networked Computers > Client Management*** link.

53. On the right side, select ***OfficeScan Server***.

54. From the ***Settings*** options, select ***Privileges and Other Settings***.

55. Click ***Privileges*** tab and select only the following options and uncheck the remaining options:

    - ***Scan Privileges > Configure Manual Scan Settings.***
    - ***Scan Privileges > Configure Real-time Scan Settings.***
    - ***Scan Privileges > Configure Scheduled Scan Settings.***
    - ***Proxy Setting Privileges > Allow the client user to configure proxy settings.***
    - ***Uninstallation > Require a password for the user to uninstall the OfficeScan Client.*** Enter a suitable password and confirm password.
    - ***Unloading > Require a password for the user to unload the OfficeScan client.*** Enter a suitable password and confirm password.

56. Click the ***Other Settings*** tab.

57. Select ***Client Security Settings > Normal*** and uncheck the remaining options.

NOTE: It is important to clear the following options.

- ***Client Self-protection > Protect OfficeScan client services.***
- ***Client Self-protection > Protect files in the OfficeScan client installation folder.***

- ***Client Self-protection > Protect OfficeScan client registry keys.***
- ***Client Self-protection > Protect OfficeScan client processes.***

58. Click ***Apply to All Clients***.

59. Click ***Close*** to close the ***Privileges and Other Settings*** screen.

60. From the left side pane, select the ***Networked Computers > Client Management link***.

61. On the right side, select ***OfficeScan Server***.

62. From the ***Settings*** options, select ***Additional Service Settings***.

63. Uncheck ***Enable service on the following operating systems*** option.

64. Click ***Apply to All Clients***.

65. Click ***Close*** to close the ***Additional Service Settings*** screen.

66. From the left side pane, select the ***Networked Computers > Global Client Settings*** link.

67. Select only the following options and uncheck the remaining options:

    - ***Scan Settings > Configure Scan settings for large compressed files.***
    - ***Scan Settings > Do not scan files in the compressed file if the size exceeds 2 MB.***
    - ***Scan Settings > In a compressed file scan only the first 100 files.***
    - ***Scan Settings > Exclude the OfficeScan server database folder from Real-time Scan.***
    - ***Scan Settings > Exclude Microsoft Exchange server folders and files from scans.***
    - ***Reserved Disk Space > Reserve 60 MB of disk space for updates.***
    - ***Proxy Configuration > Automatically detect settings.***

NOTE: It is important to clear the ***Alert Settings > Display a notification message if the client computer needs to restart to load a kernel driver***.

68. Click ***Save***.

69. From the left side pane, select the ***Updates > Networked Computers > Manual Updates*** link.

70. Select ***Manually select client*** and click ***Select***.

71. Click the appropriate domain name under ***OffceScan Server***.

72. Select client system one at a time and click ***Initiate Component Update***.

73. Click ***OK*** at the message box.

74. Click ***Log off*** and close the OfficeScan Web Console.

Trend Micro OfficeScan Post Installation Guidelines

1. On the Acquisition system(s), perform the following steps to configure Trend Micro:

   a. Click ***Start > Control Panel > Network and Sharing Center***.

   b. Click ***Change adapter settings***.

   c. Right click ***Local Area Connection*** and select ***Properties***.

d. Select ***Internet Protocol Version 4 (TCP/IPv4)*** and click ***Properties***.

e. Record the IP address _______________.

f. Close all open windows.

g. Click ***Start > Run*** and type **regedit**.

h. Navigate to ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion***.

i. On the right pane, right-click on a blank space and select ***New > String value***.

j. Type **IP Template** for the name and press **Enter**.

k. Double-click ***IP Template*** registry.

l. In ***Value*** data field, enter the Local Area Connection IP address recorded in step e.

m. Click ***OK***.

n. Close registry editor.

2. Enable the Loopback Connection. Refer to Enable Loopback Connection on page 6 for more information.

3. Configure the Computer Browser service. Refer to Configure Computer Browser Service After Anti-Virus Installation on page 7 for more information.

Trend Micro Global Settings Configurations

NOTE: The following instructions should be performed only when using the CO_2 feature with PDM in Mac-Lab/CardioLab systems. Before proceeding with the steps below, ensure that you have reviewed with IT personnel.

1. On Anti-Virus Management Console server, navigate to ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV*** folder.

2. Open the ***ofcscan.ini*** file in a text editor.

3. Under the ***Global Setting*** section, set the value of the following key to "**1**":
   [Global Setting] ***RmvTmTDI=1***

4. Save and close the ofcscan.ini file.

5. Click ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console***.

6. Enter the user name and password and click ***Log On***. The ***Summary*** screen appears.

7. Click ***Networked Computers > Global Client Settings***.

8. Click ***Save***.

9. From the left side pane, select the ***Updates > Networked Computers > Manual Update*** link.

10. Select ***Manually select clients*** and click ***Select***.

11. Click the appropriate domain name under ***OffceScan Server***.

12. Select client system one at a time and click ***Initiate Component Update***.
13. Click ***OK*** at the message box.
14. On each Acquisition system, do the following:
    a. Open registry editor.
    b. Navigate to ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc***.
    c. Ensure the ***RmvTmTDI*** registry value is set to "**1**".
    d. Navigate to ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.
    e. Delete the ***tmtdi*** registry key if it exists.
    f. Close registry editor.
    g. Restart the client systems.
    h. Login into the client systems as administrator or member of that group.
    i. On each client systems, open command prompt with administrator privilege and enter the command "***sc query tmtdi***".
    j. Ensure ***The specified service does not exist as an installed service*** message is displayed.
15. On Anti-Virus Management Console server click ***Log off*** and close the OfficeScan Web Console.

Trend Micro OfficeScan Client/Server Edition 11.0 SP1

Install Trend Micro OfficeScan Client/Server Edition on a networked Mac-Lab/CardioLab environment only. Trend Micro OfficeScan must be installed on the Anti-virus Management Console server and then deployed to Centricity Cardiology INW server and Acquisition/Review workstation as clients. Use the following instructions to install ***Trend Micro OfficeScan Client/Server Edition 11.0 SP1***.

Virus updates are the responsibility of the facility. Update the definitions regularly to ensure that the latest virus protection is on the system.

Pre-Installation Guidelines

1. The Trend Micro Anti-Virus Management Console is expected to be installed per Trend Micro instructions and working properly.
2. During installation of Trend Micro OfficeScan do the following on Anti-Virus Management Console server:
    a. Uncheck ***Enable firewall*** in the ***Anti-virus Feature*** window.
    b. Select ***No, Please do not enable assessment mode*** in the ***Anti-spyware Feature*** window.
    c. Uncheck ***Enable web reputation policy*** in the ***Web Reputation Feature*** window.

3. Trend Micro OfficeScan is not recommended when using the CO_2 feature with PDM in Mac-Lab/CardioLab systems.

4. If Trend Micro OfficeScan is required:

   a. It is recommended to configure a separate Trend Micro Anti-Virus Management Console server for the Mac-Lab/CardioLab systems. A global change to the Anti-Virus settings is required in order to use the CO_2 feature with PDM in Mac-Lab/CardioLab systems.

   b. If a separate Trend Micro Anti-Virus Management Console server cannot be configured, a change to global settings is required to the existing Trend Micro Anti-Virus Management Console server after the installation. This change will impact all client systems connected to the existing Trend Micro Anti-Virus Management Console server and should be reviewed with IT personnel before proceeding.

5. Log on as **Administrator** or a member of that group on all client systems (Acquisition, Review, and INW Server) to install the anti-virus software.

6. Disable the Loopback Connection. Refer to Disable Loopback Connection on page 6 for more information.

7. Configure the Computer Browser service. Refer to Configure Computer Browser Service Before Anti-Virus Installation on page 6 for more information.

8. The following root and intermediate certificates are required for installation on Acquisition, Review and INW client machines:

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

9. Repeat the following sub-steps to install the five required root and intermediate level certificates listed in step 8.

   a. Navigate to C***:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***.
   NOTE: On INW, navigate to C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.

   b. If the above mentioned folder path is not present, manually obtain the root and intermediate level certificates required for installation.

   c. Double click ***AddTrustExternalCARoot.crt*** to install it on the MLCL systems (Acquisition, Review and INW).

   d. Open the certificate and click ***Install Certificate***.

   e. Click ***Next*** when the ***Certificate Import Wizard*** appears.

   f. On the ***Certificate Store*** window, select ***Place all certificates in the following store*** and click ***Browse***.

   g. Check ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** and then click ***OK***.

   h. Click ***Next*** on ***Certificate Import Wizard***.

i. Click ***Finish***. ***The import was successful message*** should appear.

j. Repeat step 9 for the other certificates listed in step 8.

NOTE: Each of the certificates have an expiry date. Once the certificate has expired, they should be renewed and updated on the MLCL systems to ensure that the OfficeScan agent functions as expected.

Trend Micro OfficeScan - New Installation Deployment Steps (Preferred Push Installation Method for 11.0 SP1)

1. Click ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console***.

NOTE: Continue by selecting ***Continue to this website (not recommended)***. In the Security Alert window, check ***In the future, do not show this warning*** and click ***OK***.

2. If you receive a certificate error indicating that the site is not trusted, manage your certificates to include Trend Micro OfficeScan.
3. If prompted, install the ***AtxEnc*** add-ons. The Security Warning screen displays.
   a. Click ***Install***
4. Enter the username and password and click ***Log On***.
5. If prompted, click ***Update Now*** to install new widgets. Wait until the new widgets are updated. The update is completed screen will appear.
   a. Click ***OK***.
6. From the top menu bar, click ***Agents > Agent Installation > Remote***.
7. If prompted, install the ***AtxConsole*** add-ons. The Security Warning screen displays.
   a. Click ***Install***.
8. Double-click ***OfficeScan Server i***n the ***Remote Installation*** window. All domains will be listed under ***OfficeScan Server***.
9. Double-click the domain (Example: INW) from the list. All systems connected to the domain appear.

NOTE: If domains or systems are not listed in the ***Domains and Endpoints*** window, go to Troubleshooting Domains or Systems Not Listed in the Domains and Endpoints Window on page 62 to add them manually or run the install directly from the client machine.

10. Select the client machines (Acquisition, Review, and INW Server) and click ***Add***.
11. Type the <domain name>\username and password and click ***Log on***.
12. Select the client machines (Acquisition, Review, and INW Server) one at a time from the ***Selected Endpoints*** pane and click ***Install***.
13. Click ***OK*** at the confirmation box.
14. Click ***OK*** at the ***Number of clients to which notifications were sent*** message box.

15. Restart all the client machines (Acquisition, Review, and INW Server) and Log in as Administrator or a member of that group on all client machines and wait until the Trend Micro OfficeScan icon in system tray changes to blue with a green tick mark symbol.

16. Click the ***Log Off*** link to close the ***OfficeScan Web Console***.

Trend Micro OfficeScan Server Console Configuration for 11.0 SP1

1. Select ***Start > All Programs > TrendMicro Office Scan server <servername> > Office Scan Web Console***. The ***Trend Micro OfficeScan Login*** screen appears.

2. Enter the user name and password and click ***Login***. The ***Summary*** screen appears.

3. From the top pane, select the ***Agents > Agent Management*** link.

4. On the left side, select ***OfficeScan Server***.

5. From the ***Settings*** options, select ***Scan Settings > Manual Scan Settings***. The ***Manual Scan Settings*** screen appears.

6. Click the ***Target*** tab and select only the following options and uncheck the remaining options:
   - ***Files to Scan > File types scanned by IntelliScan.***
   - ***Scan Settings > Scan compressed files.***
   - ***Scan Settings > Scan OLE objects.***
   - ***Virus/Malware Scan Settings Only > Scan boot area.***
   - ***CPU Usage > Low.***
7. Click the Scan Exclusion tab and select only the following options and uncheck the remaining options:
   - ***Scan Exclusion > Enable scan exclusion.***
   - ***Scan Exclusion > Apply scan exclusion settings to all scan types.***
   - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed.***
   - ***Select Adds path*** to from the drop-down under ***Saving the officescan agent's exclusion list does the following:***
   - Enter the **C:\Program Files (x86)\GE Healthcare\MLCL\**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:\** and **G:\** folders one at a time click **+**.
8. Click ***Apply to All Agents***.

9. Click ***OK*** at the ***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?*** message.

10. Click ***Close*** to close the ***Manual Scan Settings*** screen.

11. From the top pane, select the ***Agent > Agent Management*** link.

12. On the left side, select ***OfficeScan*** Server.

13. From the ***Settings*** options, select ***Scan Settings > Real-time Scan Settings***. The ***Real-time Scan Settings*** screen appears.

14. Click the ***Target*** tab and select only the following options and uncheck the remaining options:

- ***Real-Time Scan Settings > Enable virus/malware scan.***
- ***Real-Time Scan Settings > Enable spyware/grayware scan.***
- ***Files to Scan > File types scanned by IntelliScan.***
- ***Scan Settings > Scan compressed files.***
- ***Scan Settings > Scan OLE objects.***
- ***Virus/Malware Scan Settings Only > Enable IntelliTrap.***

15. Click the Scan Exclusion tab and select only the following options and uncheck the remaining options:

    - ***Scan Exclusion > Enable scan exclusion.***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types.***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed.***
    - Make sure the ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:\*** and ***G:\*** folder paths are present in the ***Exclusion List***.

16. Click the ***Action*** tab.
17. Keep the default settings and uncheck the following options:

    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected.***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/grayware is detected.***

18. Click ***Apply to All Agents***.
19. Click ***Close*** to close the ***Real-time Scan Settings*** screen.
20. From the top pane, select the ***Agents > Agent Management*** link.
21. On the left side, select ***OfficeScan Server***.
22. From the ***Settings*** options, select ***Scan Settings > Scheduled Scan Settings***. The ***Scheduled Scan Settings*** screen appears.
23. Click the ***Target*** tab and select only the following options and uncheck the remaining options:

    - ***Scheduled Scan Settings > Enable virus/malware scan.***
    - ***Scheduled Scan Settings > Enable spyware/grayware scan.***
    - ***Schedule > Weekly, every Sunday, Start time: 00:00 hh:mm.***
    - ***Files to Scan > File types scanned by IntelliScan.***
    - ***Scan Settings > Scan compressed files.***
    - ***Scan Settings > Scan OLE objects.***
    - ***Virus/Malware Scan Settings Only > Scan boot area.***
    - ***CPU Usage > Low.***

24. Click the ***Scan Exclusion*** tab and select only the following options and uncheck the remaining options:

    - ***Scan Exclusion > Enable scan exclusion.***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types.***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed.***

- Make sure the ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:\*** and ***G:\*** folder paths are present in the Exclusion List.

25. Click the ***Action*** tab.
26. Keep the default settings and uncheck the following options:
    - ***Virus/Malware > Display a notification message on the endpoints when virus/ malware is detected.***
    - ***Spyware/Grayware > Display a notification message on the endpoints when spyware/grayware is detected.***
27. Click ***Apply to All Agents***.
28. Click ***Close*** to close the ***Scheduled Scan Settings*** screen.
29. From the top pane, select the ***Agents > Agent Management*** link.
30. On the left side, select ***OfficeScan Server***.
31. From the ***Settings*** options, select ***Scan Settings > Scan Now Settings***. The ***Scan Now Settings*** screen appears.
32. Click the ***Target*** tab and select only the following options and uncheck the remaining options:
    - ***Scan Now Settings > Enable virus/malware scan.***
    - ***Scan Now Settings > Enable spyware/grayware scan.***
    - ***Files to Scan > File types scanned by IntelliScan.***
    - ***Scan Settings > Scan compressed files.***
    - ***Scan Settings > Scan OLE objects.***
    - ***Virus/Malware Scan Settings Only > Scan boot area.***
    - ***CPU Usage > Low.***
33. Click the ***Scan Exclusion*** tab and select only the following options and uncheck the remaining options:
    - ***Scan Exclusion > Enable scan exclusion.***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types.***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed.***
    - Make sure the ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:\*** and ***G:\*** folder paths are present in the Exclusion List.
34. Click ***Apply to All Agents***.
35. Click ***Close*** to close the ***Scan Now Settings*** screen.
36. From the top pane, select the ***Agents > Agent Management*** link.
37. On the left side, select ***OfficeScan Server***.
38. From the ***Settings*** options, select ***Web Reputation Settings***. The ***Web Reputation Settings*** screen appears.
39. Click the ***External Agents*** tab and uncheck ***Enable Web reputation policy on the following operating systems***, if selected already during installation.

40. Click the ***Internal Agents*** tab and uncheck ***Enable Web reputation policy on the following operating systems***, if selected already during installation.

41. Click ***Apply to All Agents***.

42. Click ***Close*** to close the ***Web Reputation*** screen.

43. From the top pane, select the ***Agents > Agent Management*** link.

44. On the left side, select ***OfficeScan Server***.

45. From the ***Settings*** options, select ***Behavior Monitoring Settings***. The ***Behavior Monitoring Settings*** screen appears.

46. Uncheck the ***Enable Malware Behavior Blocking for known and potential threats*** and ***Enable Event Monitoring*** options.

47. Click ***Apply to All Agents***.

48. Click ***Close*** to close the ***Behavior Monitoring*** screen.

49. From the top pane, select the ***Agents > Agent Management*** link.

50. On the left side, select ***OfficeScan Server***.

51. From the ***Settings*** options, select ***Device Control Settings***. The ***Device Control Settings*** screen appears.

52. Click the ***External Agents*** tab and uncheck the following options:

    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access.***
    - ***Block the AutoRun function on USB storage devices.***

53. Click the ***Internal Agents*** tab and uncheck the following options:

    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access.***
    - ***Block the AutoRun function on USB storage devices.***

54. Click ***Apply to All Agents***.

55. Click ***Close*** to close the ***Device Control Settings*** screen.

56. From the ***Settings*** options, again select ***Device Control Settings***. The ***Device Control Settings*** screen appears.

57. Click the ***External Agents*** tab and uncheck ***Enable Device Control***.

58. Click the ***Internal Agents*** tab and uncheck ***Enable Device Control***.

59. Click ***Apply to All Agents***.

60. Click ***Close*** to close the ***Device Control Settings*** screen.

61. From the top pane, select the ***Agents > Agent Management*** link.

62. On the left side, select ***OfficeScan Server***.

63. From the ***Settings*** options, select ***Privileges and Other Settings***.

64. Click ***Privileges*** tab and select only the following options and uncheck the remaining options:

- ***Scans > Configure Manual Scan Settings.***
- ***Scans > Configure Real-time Scan Settings.***
- ***Scans > Configure Scheduled Scan Settings.***
- ***Proxy Settings > Allow users to configure proxy settings.***
- ***Uninstallation > Requires a password.*** Enter a suitable password and confirm password.
- ***Unloading and Unlock > Requires a password.*** Enter a suitable password and confirm password.

65. Click the ***Other Settings*** tab.
66. Select ***OfficeScan Agent Security Settings > Normal: Allow users to access OfficeScan agent files and registries*** and uncheck the remaining options.

NOTE: It is important to clear the following options.

- ***OfficeScan Agent Self-protection > Protect OfficeScan agent services.***
- ***OfficeScan Agent Self-protection > Protect files in the OfficeScan agent installation folder.***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent registry keys.***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent processes.***

67. Click ***Apply to All Agents***.
68. Click ***Close*** to close the ***Privileges and Other Settings*** screen.
69. From the top pane, select the ***Agents > Agent Management link***.
70. On the left side, select ***OfficeScan Server***.
71. From the ***Settings*** options, select ***Additional Service Settings***.
72. Uncheck ***Enable service on the following operating systems*** option.
73. Click ***Apply to All Agents***.
74. Click ***Close*** to close the ***Additional Service Settings*** screen.
75. From the top pane, select the ***Agents > Global Agent Settings*** link.
76. Select only the following options and uncheck the remaining options:

- ***Scan Settings for Large Compressed Files > Configure Scan settings for large compressed files.***
- ***Scan Settings for Large Compressed Files > Do not scan files in the compressed file if the size exceeds 2 MB***. Follow this for ***Real-Time Scan*** and ***Manual Scan/ Schedule Scan/Scan Now***.
- ***Scan Settings for Large Compressed Files > In a compressed file scan only the first 100 files.*** Follow this for ***Real-Time Scan*** and ***Manual Scan/Schedule Scan/Scan Now***.
- ***Scan Settings > Exclude the OfficeScan server database folder from Real-time Scan.***
- ***Scan Settings > Exclude Microsoft Exchange server folders and files from scans.***
- ***Reserved Disk Space > Reserve 60 MB of disk space for updates.***
- ***Proxy Configuration > Automatically detect settings.***

NOTE: It is important to clear the ***Alert Settings > Display a notification message*** if the endpoint needs to restart to load a Kernel mode driver.

77. Click ***Save***.

78. From the top pane, select the ***Updates > Agents > Manual Updates*** link.

79. Select ***Manually select agents*** and click ***Select***.

80. Double-click the appropriate domain name under ***OffceScan Server***.

81. Select client system one at a time and click ***Initiate Update***.

82. Click ***OK*** at the message box.

83. Click ***Log off*** and close the OfficeScan Web Console.

Trend Micro Global Settings Configurations

NOTE: The following instructions should be performed only when using the CO_2 feature with PDM in Mac-Lab/CardioLab systems. Before proceeding with the steps below, ensure that you have reviewed with IT personnel.

1. On Anti-Virus Management Console server, navigate to ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV*** folder.
2. Open the ***ofcscan.ini*** file in a text editor.
3. Under the Global Setting section, set the value of the following key to "**1**": [Global Setting] ***RmvTmTDI=1***
4. Save and close the ofcscan.ini file.
5. Click ***Start > All Programs > TrendMicro OfficeScan server - <server name> > OfficeScan Web Console***.
6. Enter the user name and password and click ***Log On***. The ***Dashboard*** screen appears.
7. Click ***Agents > Global Agent Settings***.
8. Click ***Save***.
9. From the left side pane, select the ***Updates > Agents > Manual Update*** link.
10. Select ***Manually select clients*** and click ***Select***.
11. Click the appropriate domain name under ***OfficeScan Server***.
12. Select client system one at a time and click ***Initiate Update***.
13. Click ***OK*** at the message box.
14. On each Acquisition system, do the following:
    a. Open registry editor.

    b. Navigate to ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc.***

    c. Ensure the ***RmvTmTDI*** registry value is set to "***1***".

    d. Navigate to ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***.

e. Delete the ***tmtdi*** registry key if it exists.

f. Close registry editor.

g. Restart the client systems.

h. Login into the client systems as administrator or member of that group.

i. On each client systems, open command prompt with administrator privilege and enter the command "***sc query tmtdi***".

j. Ensure ***The specified service does not exist as an installed service*** message is displayed.

15. On Anti-Virus Management Console server click ***Log off*** and close the OfficeScan Web Console.

Trend Micro OfficeScan Post Installation Guidelines

1. Enable the Loopback Connection. Refer to Enable Loopback Connection on page 6 for more information.
2. Configure the Computer Browser service. Refer to Configure Computer Browser Service After Anti-Virus Installation on page 7 for more information.

Trend Micro OfficeScan Client/Server Edition XG 12.0

Installation Overview

Install Trend Micro OfficeScan Client/Server Edition on a networked Mac-Lab/CardioLab environment only. Trend Micro OfficeScan must be installed on the Anti-virus Management Console server and then deployed to Centricity Cardiology INW server and Acquisition/Review workstation as clients. Use the following instructions to install ***Trend Micro OfficeScan Client/ Server Edition XG 12.0***.

Virus updates are the responsibility of the facility. Update the definitions regularly to ensure that the latest virus protection is on the system.

Pre-Installation Guidelines

NOTE: Internet Explorer 10 is the minimum IE browser required to run OfficeScan manager.

1. The Trend Micro Anti-Virus Management Console is expected to be installed per Trend Micro instructions and working properly.
2. During installation of Trend Micro OfficeScan do the following on Anti-Virus Management Console server:

   a. Uncheck ***Enable firewall*** in the ***Anti-virus Feature*** window.

   b. Select ***No, Please do not enable assessment mode*** in the ***Anti-spyware Feature*** window.

   c. Uncheck ***Enable web reputation policy*** in the ***Web Reputation Feature*** window.

3. Log on as **Administrator** or a member of that group on all client systems (Acquisition, Review, and INW Server) to install the anti-virus software.

4. Disable the Loopback Connection. Refer to Disable Loopback Connection on page 6 for more information.

5. Configure the Computer Browser service. Refer to Configure Computer Browser Service Before Anti-Virus Installation on page 6 for more information.

6. The following root and intermediate certificates are required for installation on Acquisition, Review and INW client machines:

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

7. Repeat the following sub-steps to install the five required root and intermediate level certificates listed in step 6.

   a. Navigate to C***:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***.
   NOTE: On INW, navigate to C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro.

   b. If the above mentioned folder path is not present, manually obtain the root and intermediate level certificates required for installation.

   c. Double click ***AddTrustExternalCARoot.crt*** to install it on the MLCL systems (Acquisition, Review and INW).

   d. Open the certificate and click ***Install Certificate***.

   e. Click ***Next*** when the ***Certificate Import Wizard*** appears.

   f. On the ***Certificate Store*** window, select ***Place all certificates in the following store*** and click ***Browse***.

   g. Check ***Show physical stores > Trusted Root Certification Authorities > Local Computer*** and then click ***OK***.

   h. Click ***Next*** on ***Certificate Import Wizard***.

   i. Click ***Finish***. ***The import was successful message*** should appear.

   j. Repeat step 7 for the other certificates listed in step 6.

NOTE: Each of the certificates have an expiry date. Once the certificate has expired, they should be renewed and updated on the MLCL systems to ensure that the OfficeScan agent functions as expected.

Trend Micro OfficeScan - New Installation Deployment Steps (Preferred Push Installation Method for 12.0)

1. Click ***Start > All Programs > TrendMicro OfficeScan server - <server name> > Office Scan Web Console***.

NOTE: Continue by selecting ***Continue to this website (not recommended)***. In the Security Alert window, check ***In the future, do not show this warning*** and click ***OK***.

2. If you receive a certificate error indicating that the site is not trusted, manage your certificates to include Trend Micro OfficeScan.

3. If prompted, install the ***AtxEnc*** add-ons. The Security Warning screen displays.

   a. Click ***Install***

4. Enter the username and password and click ***Log On***.

5. If prompted, click ***Update Now*** to install new widgets. Wait until the new widgets are updated. The update is completed screen will appear.

   a. Click ***OK***.

6. From the top menu bar, click ***Agents > Agent Installation > Remote***.

7. If prompted, install the ***AtxConsole*** add-ons. The Security Warning screen displays.

   a. Click ***Install***.

8. Double-click ***My Company*** in the ***Remote Installation*** window. All domains will be listed under ***OfficeScan Server***.

9. Double-click the domain (Example: INW) from the list. All systems connected to the domain appear.

NOTE: If domains or systems are not listed in the ***Domains and Endpoints*** window, go to Troubleshooting Domains or Systems Not Listed in the Domains and Endpoints Window on page 62 to add them manually or run the install directly from the client machine.

10. Select the client machines (Acquisition, Review, and INW Server) and click ***Add***.

11. Type the <domain name>\username and password and click ***Log on***.

12. Select the client machines (Acquisition, Review, and INW Server) one at a time from the ***Selected Endpoints*** pane and click ***Install***.

13. Click ***Yes*** at the confirmation box.

14. Click ***OK*** at the ***Number of agents to which notifications were sent*** message box.

15. Restart all the client machines (Acquisition, Review, and INW Server) and Log in as Administrator or a member of that group on all client machines and wait until the Trend Micro OfficeScan icon in system tray changes to blue with a green tick mark symbol.

16. Click the ***Log Off*** link to close the ***OfficeScan Web Console***.

Trend Micro OfficeScan Server Console Configuration for 12.0

1. Select ***Start > All Programs > TrendMicro Office Scan server <servername> > Office Scan Web Console***. The ***Trend Micro OfficeScan Login*** screen appears.

2. Enter the user name and password and click ***Login***. The ***Summary*** screen appears.

3. From the top pane, select the ***Agents > Agent Management*** link.

4. On the left side, select ***OfficeScan Server***.

5. From the ***Settings*** options, select ***Scan Settings > Manual Scan Settings***. The ***Manual Scan Settings*** screen appears.

6. Click the ***Target*** tab and select only the following options and uncheck the remaining options:

   - ***Files to Scan > File types scanned by IntelliScan.***
   - ***Scan Settings > Scan compressed files.***
   - ***Scan Settings > Scan OLE objects.***
   - ***Virus/Malware Scan Settings Only > Scan boot area.***
   - ***CPU Usage > Low.***

7. Click the Scan Exclusion tab and select only the following options and uncheck the remaining options:

   - ***Scan Exclusion > Enable scan exclusion.***
   - ***Scan Exclusion > Apply scan exclusion settings to all scan types.***
   - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed and select Add path to agent Computers Exclusion list.***
   - ***Select Adds path*** to from the drop-down under ***Saving the officescan agent's exclusion list does the following:***
   - Enter the **C:\Program Files (x86)\GE Healthcare\MLCL\**, **C:\Program Files\GE Healthcare\MLCL\, D:\GEData\Studies**, **E:\** and **G:\** folders one at a time click ***Add***.

8. Click ***Apply to All Agents***.

9. Click ***OK*** at the ***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?*** message.

10. Click ***Close*** to close the ***Manual Scan Settings*** screen.

11. From the top pane, select the ***Agent > Agent Management*** link.

12. On the left side, select ***OfficeScan*** Server.

13. From the ***Settings*** options, select ***Scan Settings > Real-time Scan Settings***. The ***Real-time Scan Settings*** screen appears.

14. Click the ***Target*** tab and select only the following options and uncheck the remaining options:

   - ***Real-Time Scan Settings > Enable virus/malware scan.***
   - ***Real-Time Scan Settings > Enable spyware/grayware scan.***
   - ***Files to Scan > File types scanned by IntelliScan.***
   - ***Scan Settings > Scan compressed files.***
   - ***Scan Settings > Scan OLE objects.***
   - ***Virus/Malware Scan Settings Only > Enable IntelliTrap.***

15. Click the Scan Exclusion tab and select only the following options and uncheck the remaining options:

   - ***Scan Exclusion > Enable scan exclusion.***
   - ***Scan Exclusion > Apply scan exclusion settings to all scan types.***
   - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed.***

- Make sure the ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL, D:\GEData\Studies***, ***E:\*** and ***G:\*** folder paths are present in the ***Exclusion List***.

16. Click the ***Action*** tab.
17. Keep the default settings and uncheck the following options:
    - ***Virus/Malware > Display a notification message on endpoints when virus/malware is detected.***
    - ***Spyware/Grayware > Display a notification message on endpoints when spyware/ grayware is detected.***
18. Click ***Apply to All Agents***.
19. Click ***Close*** to close the ***Real-time Scan Settings*** screen.
20. From the top pane, select the ***Agents > Agent Management*** link.
21. On the left side, select ***OfficeScan Server***.
22. From the ***Settings*** options, select ***Scan Settings > Scheduled Scan Settings***. The ***Scheduled Scan Settings*** screen appears.
23. Click the ***Target*** tab and select only the following options and uncheck the remaining options:
    - ***Scheduled Scan Settings > Enable virus/malware scan.***
    - ***Scheduled Scan Settings > Enable spyware/grayware scan.***
    - ***Schedule > Weekly, every Sunday, Start time: 00:00 hh:mm.***
    - ***Files to Scan > File types scanned by IntelliScan.***
    - ***Scan Settings > Scan compressed files.***
    - ***Scan Settings > Scan OLE objects.***
    - ***Virus/Malware Scan Settings Only > Scan boot area.***
    - ***CPU Usage > Low.***
24. Click the Scan Exclusion tab and select only the following options and uncheck the remaining options:
    - ***Scan Exclusion > Enable scan exclusion.***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types.***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed.***
    - Make sure the ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:\*** and ***G:\*** folder paths are present in the Exclusion List.
25. Click the ***Action*** tab.
26. Keep the default settings and uncheck the following options:
    - ***Virus/Malware > Display a notification message on the endpoints when virus/ malware is detected.***
    - ***Spyware/Grayware > Display a notification message on the endpoints when spyware/grayware is detected.***
27. Click ***Apply to All Agents***.
28. Click ***Close*** to close the ***Scheduled Scan Settings*** screen.

29. From the top pane, select the ***Agents > Agent Management*** link.

30. On the left side, select ***OfficeScan Server***.

31. From the ***Settings*** options, select ***Scan Settings > Scan Now Settings***. The ***Scan Now Settings*** screen appears.

32. Click the ***Target*** tab and select only the following options and uncheck the remaining options:

    - ***Scan Now Settings > Enable virus/malware scan.***
    - ***Scan Now Settings > Enable spyware/grayware scan.***
    - ***Files to Scan > File types scanned by IntelliScan.***
    - ***Scan Settings > Scan compressed files.***
    - ***Scan Settings > Scan OLE objects.***
    - ***Virus/Malware Scan Settings Only > Scan boot area.***
    - ***CPU Usage > Low.***

33. Click the ***Scan Exclusion*** tab and select only the following options and uncheck the remaining options:

    - ***Scan Exclusion > Enable scan exclusion.***
    - ***Scan Exclusion > Apply scan exclusion settings to all scan types.***
    - ***Scan Exclusion List (Directories) > Exclude directories where Trend Micro products are installed.***
    - Make sure the ***C:\Program Files (x86)\GE Healthcare\MLCL***, ***C:\Program Files \GE Healthcare\MLCL***, ***D:\GEData\Studies***, ***E:\*** and ***G:\***

34. Click ***Apply to All Agents***.

35. Click ***Close*** to close the ***Scan Now Settings*** screen.

36. From the top pane, select the ***Agents > Agent Management*** link.

37. On the left side, select ***OfficeScan Server***.

38. From the ***Settings*** options, select ***Web Reputation Settings***. The ***Web Reputation Settings*** screen appears.

39. Click the ***External Clients*** tab and uncheck ***Enable Web reputation policy on the following operating systems***, if selected already during installation.

40. Click the ***Internal Agents*** tab and uncheck ***Enable Web reputation policy on the following operating systems***, if selected already during installation.

41. Click ***Apply to All Agents***.

42. Click ***Close*** to close the ***Web Reputation*** screen.

43. From the top pane, select the ***Agents > Agent Management*** link.

44. On the left side, select ***OfficeScan Server***.

45. From the ***Settings*** options, select ***Behavior Monitoring Settings***. The ***Behavior Monitoring Settings*** screen appears.

46. Uncheck the ***Enable Malware Behavior Blocking*** and ***Enable Event Monitoring*** options.

47. Click ***Apply to All Agents***.

48. Click ***Close*** to close the ***Behavior Monitoring*** screen.

49. From the top pane, select the ***Agents > Agent Management*** link.

50. On the left side, select ***OfficeScan Server***.

51. From the ***Settings*** options, select ***Device Control Settings***. The ***Device Control Settings*** screen appears.

52. Click the ***External Agents*** tab and uncheck the following options:

    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access.***
    - ***Block the AutoRun function on USB storage devices.***
    - ***Enable Device Control.***

53. Click the ***Internal Agents*** tab and uncheck the following options:

    - ***Notification > Display a notification message on endpoints when OfficeScan detects unauthorized device access.***
    - ***Block the AutoRun function on USB storage devices.***
    - ***Enable Device Control.***

54. Click ***Apply to All Agents***.

55. Click ***Close*** to close the ***Device Control Settings*** screen.

56. From the ***Settings*** options, again select ***Device Control Settings***. The ***Device Control Settings*** screen appears.

57. Click the ***External Agents*** tab and uncheck ***Enable Device Control***.

58. Click the ***Internal Agents*** tab and uncheck ***Enable Device Control***.

59. Click ***Apply to All Agents***.

60. Click ***Close*** to close the ***Device Control Settings*** screen.

61. From the left side pane, select the ***Agents > Agent Management*** link.

62. On the left side, select ***OfficeScan Server***.

63. From the ***Settings*** options, select ***Privileges and Other Settings***.

64. Click ***Privileges*** tab and select only the following options and uncheck the remaining options:

    - ***Scan Privileges > Configure Manual Scan Settings.***
    - ***Scan Privileges > Configure Real-time Scan Settings.***
    - ***Scan Privileges > Configure Scheduled Scan Settings.***
    - ***Proxy Setting Privileges > Allow the agent user to configure proxy settings.***
    - ***Uninstallation > Requires a password.*** Enter a suitable password and confirm password.
    - ***Unload and Unlock > Requires a password.*** Enter a suitable password and confirm password.

65. Click the ***Other Settings*** tab.

66. Uncheck all options.

NOTE: It is important to clear the following options.

- ***OfficeScan Agent Self-protection > Protect OfficeScan agent services.***
- ***OfficeScan Agent Self-protection > Protect files in the OfficeScan agent installation folder.***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent registry keys.***
- ***OfficeScan Agent Self-protection > Protect OfficeScan agent processes.***

67. Click ***Apply to All Agents***.
68. Click ***Close*** to close the ***Privileges and Other Settings*** screen.
69. From the top pane, select the ***Agents > Agent Management link***.
70. On the left side, select ***OfficeScan Server***.
71. From the ***Settings*** options, select ***Additional Service Settings***.
72. Uncheck ***Enable service on the following operating systems*** option.
73. Click ***Apply to All Agents***.
74. Click ***Close*** to close the ***Additional Service Settings*** screen.
75. From the top pane, select the ***Agents > Global Agent Settings*** link.
76. Select only the following options and uncheck the remaining options:
    - ***Scan Settings for Large Compressed Files > Do not scan files in the compressed file if the size exceeds 2 MB***. Follow this for ***Real-Time Scan*** and ***Manual Scan/Schedule Scan/Scan Now***.
    - ***Scan Settings for Large Compressed Files > In a compressed file scan only the first 100 files.*** Follow this for ***Real-Time Scan*** and ***Manual Scan/Schedule Scan/Scan Now***.
    - ***Scan Settings > Exclude the OfficeScan server database folder from Real-time Scan.***
    - ***Scan Settings > Exclude Microsoft Exchange server folders and files from scans.***
77. Click ***Save***.
78. From the top pane, select the ***Updates > Agents > Manual Updates*** link.
79. Select ***Manually select agents*** and click ***Select***.
80. Double-click the appropriate domain name under ***OffceScan Server***.
81. Select client system one at a time and click ***Initiate Update***.
82. Click ***OK*** at the message box.
83. Click ***Log off*** and close the OfficeScan Web Console.

Trend Micro OfficeScan Post Installation Guidelines

1. Enable the Loopback Connection. Refer to Enable Loopback Connection on page 6 for more information.
2. Configure the Computer Browser service. Refer to Configure Computer Browser Service After Anti-Virus Installation on page 7 for more information.

Troubleshooting Domains or Systems Not Listed in the Domains and Endpoints Window

During the preferred push installation methods for both Trend Micro OfficeScan Client/Server Edition 11.0 SP1 and Trend Micro OfficeScan Client/Server Edition XG 12.0, the domains and systems must be listed to push the installation to the system. These steps give you two options to install the anti-virus software on the clients (Acquisition, Review and INW).

For 11.0 SP1, see Trend Micro OfficeScan - New Installation Deployment Steps (Preferred Push Installation Method for 11.0 SP1) on page 47.
For 12.0, see Trend Micro OfficeScan - New Installation Deployment Steps (Preferred Push Installation Method for 12.0) on page 55.

1. Use the IP addresses of client machines (Acquisition, Review and INW) on the management console and do the following:

   a. Enter the IP of each of the client systems in the ***Search for endpoints*** box one at a time and press ***Enter***.

   b. Provide ***<domain name>\username*** and password and click ***Log on***.

   c. Choose one of the following steps based on your Trend Micro version:

      i. For 11.0 SP1, return to step 10 on page 47.

      ii. For 12.0, return to step 10 on page 56.

2. If you do not know the IP address of the systems, or the previous option fails, go to each client machine (Acquisition, Review, and INW Server) and do the following:

   a. Log in as **Administrator** or a member of that group on all client machines.

   b. Click ***Start > Run***.

   c. Type **\\*<Anti-Virus Management Console_server_IP_address>*** and press ***Enter***. When prompted enter the administrator username and password.

   d. Navigate to **\\*<Anti-Virus Management Console_server_IP _address>\ofsscan*** and double-click ***AutoPcc.exe***. When prompted enter the administrator username and password.

   e. Restart the client systems when the installation is complete.

   f. Log in as **Administrator** or a member of that group on all client machines and wait until the Trend Micro OfficeScan icon in system tray changes to blue.

   g. Choose one of the following steps based on your Trend Micro version:

      i. For 11.0 SP1, see Trend Micro OfficeScan Server Console Configuration for 11.0 SP1 on page 48.

      ii. For 12.0, see Trend Micro OfficeScan Server Console Configuration for 12.0 on page 56.