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

Mac-Lab/CardioLab Software Version 7.1

Introduction

Anti-virus software is an important part of maintaining system stability and performance. The MLCL system has been designed to operate with most commercial Anti-Virus/Whitelisting applications that can be installed per the guideline provided below.

Document Use

Use this document to install anti-virus/whitelisting software for the Mac-Lab/CardioLab v7.1 system.

Revision History

Revision	Date	Comments
A	16 April 2020	Initial release.
B	24 September 2021	Added **Mac-Lab/CardioLab Folders Exclusion** section. Referenced **Mac-Lab/CardioLab Folders Exclusion** section to exclude Mac-Lab/CardioLab folders in all antivirus software sections.

Getting Started

Anti-Virus Requirements

⚠

WARNING: ANTI-VIRUS SOFTWARE INSTALLATION REQUIRED

The System is delivered with the Microsoft Defender anti-virus application active to ensure some level of protection during system setup. Customers may choose to leave this software active or replace it with a product of their choosing. Lack of virus protection could lead to system instability or failure.

Minimum requirements to install Anti-Virus:

- It is the customer's responsibility to acquire and maintain virus protection software.
- It is the customer's responsibility to refer to the installation instructions provided by the manufacturer of the anti-virus or whitelisting security software.
- For anti-virus or whitelisting security software installation:
  - If the customer choses to install any of the reference anti-virus software, it is their responsibility to follow the instructions under Reference Anti-Virus Software section for details.
  - If the customer wants to install a non-reference anti-virus or whitelisting security software, contact GE Service Representative.
- The customer is responsible for updating anti-virus definition files.
- If a virus is found contact the facility System Administrator and GE Technical Support.
- Log in as a user who is a member of the local administrators group on the system to perform the activities in this document.

A checkout procedure present in 5123010-1EN Service manual shall be followed post-installation and configuration of non-reference Antivirus/security program. It shall be followed every time when a non-reference Antivirus/security setting (automatic update/upgrade or any other settings) are changed.

Most of the Anti-Virus or Whitelisting security software can be installed on MLCL systems with guidance from GE service representative. A checkout procedure must be performed post installation. For convenience, we have created specific installation instructions for common versions of Anti-Virus software. The list of anti-virus software is present in the below section. The anti-virus versions and their configurations are provided in detail in the below sections.

Reference Anti-Virus Software

⚠

WARNING: SYSTEM INSTABILITY

Do not install or use anti-virus software that do not meet the requirements mentioned in the above section. Doing so may result in system instability or failure.

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

Refer to the below sections for installation instructions which have been validated to meet the compatibility requirements for use with MLCL systems for the specific Anti-Virus versions below.

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 14
McAfee ePolicy Orchestrator (with McAfee VirusScan Enterprise)	English, French, German, Italian, Spanish, Swedish, Norwegian, Danish, Dutch, Chinese, Japanese	5.10.0 w/ Patch 2428
Symantec EndPoint Protection	English, French, German, Italian, Spanish, Swedish, Norwegian, Danish, Dutch, Chinese, Japanese	14.2.2 MP1
Trend Micro OfficeScan Client/Server Edition	English, French, German, Italian, Spanish, Swedish, Norwegian, Danish, Dutch, Chinese, Japanese	XG SP1 w/ Critical patch 5474

Anti-virus Management Console Server Configuration

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

1.. Hospital Domain Controller Environment - Anti-virus Management Console SVR not in Hospital Domain Controller Domain

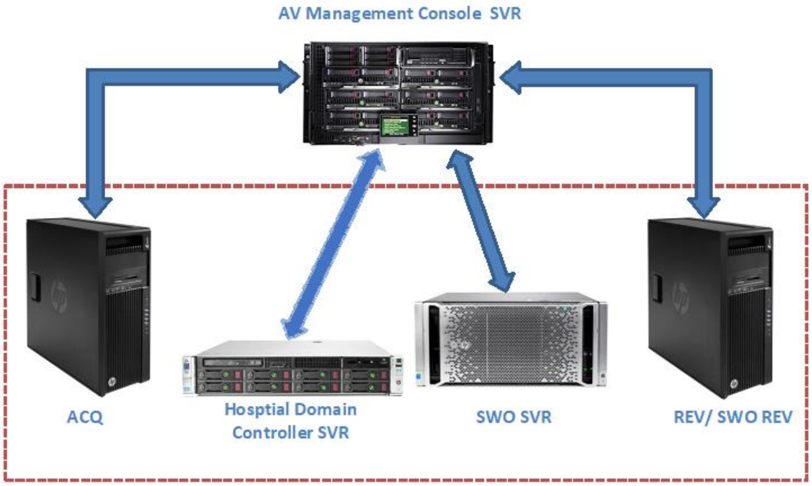
    ■ Communication Type - 1 <Different network with different subnet mask>

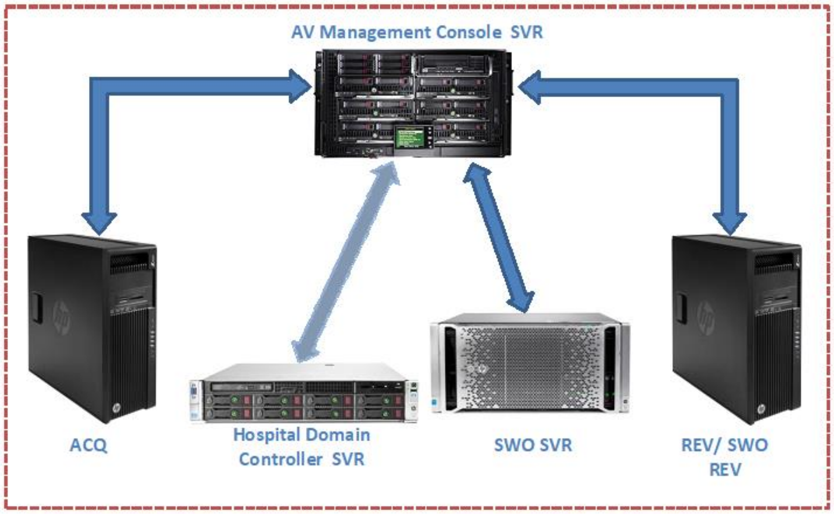
2. Hospital Domain Controller Environment - Anti-virus Management Console SVR in Hospital Domain Controller Domain

    ■ 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.

Hospital Domain Controller Environment Block Diagram





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.

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

Mac-Lab/CardioLab Folders Exclusion

Following Mac-Lab/CardioLab folders needs to be excluded in the antivirus software based on the system type:

INW Server	Acquisition	Review
<InstallDir>	<InstallDir>	<InstallDir>
<DataDir>Logs	<DataDir>Studies	<DataDir>Studies
<DataDir>Studies	E:\	G:\
<DataDir>Temp	G:\	

Where:

- **InstallDir:** C:\Program Files\GE Healthcare\MLCL\
- **DataDir:** C:\GEData\

  On INW server, the default DataDir location is C:\GEData. The Mac-Lab/CardioLab installation allows user to choose the DataDir drive during installation. So, the drive letter for GEData folder may change depending on the driver letter selected during Mac-Lab/CardioLab installation.

Note:

- **<DataDir>Logs** and **<DataDir>Temp** folders needs to be excluded only when the **CVIS integration** is enabled in **INW server**.
- When excluding the folders in antivirus software, full folder name (**example**: C:\Program Files\GE Healthcare\MLCL\ or D:\GEData\Logs\) should be entered or selected in the folder exclusion window.
- If management console is used to deploy and manage the antivirus software, applicable Mac-Lab/CardioLab folders should be excluded from the above table.
- The folders listed in the above table need to be excluded regardless of the antivirus software including **Windows Defender**.

Anti-Virus Installation Instructions

Click the anti-virus software you want to install:

- Symantec EndPoint Protection on page 9
- McAfee VirusScan Enterprise on page 15
- McAfee ePolicy Orchestrator on page 18
- Trend Micro OfficeScan Client/Server Edition on page 27

Anti-Virus Software Common Installation Procedures

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

Configure Computer Browser Service Before Anti-Virus Installation

Check the Computer Browser service (if available) setting on networked INW, 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 ***Domain (current profile).***
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. Record the ***Startup type*** for Computer Browser service ______.
10. Make sure the ***Startup type*** is set to ***Automatic***. If it's not set to Automatic, change it and click ***Start***.
11. Click ***OK***.
12. Close the ***Services*** window.

Configure Remote Registry Service Before Anti-Virus Installation

Check the Remote registry service setting on networked Acquisition 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 ***Remote Registry*** service.
4. Record the ***Startup type*** for Remote Registry service ______.
5. Make sure the ***Startup type*** is set to ***Automatic***. If it's not set to Automatic, change it and click ***Start***.

5. Click ***OK***.
6. Close the ***Services*** window.

Configure Computer Browser After Anti-Virus Installation

Check the Computer browser service (if available) setting on networked INW, Acquisition 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 the state as recorded in section Configure Computer Browser Before Anti-Virus Installation step 9.
5. Click ***OK***.
6. Close the ***Services*** window.

Configure Remote Registry Service After Anti-Virus Installation

Check the Remote registry service setting on networked Acquisition 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 ***Remote Registry*** service.
4. Change the ***Startup type*** to the state as recorded in section Configure Remote Registry Before Anti-Virus Installation step 4.
5. Click ***OK***.
6. Close the ***Services*** window.

Symantec EndPoint Protection (14.2.2 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 a user who is a member of the local administrator group on all client systems (Acquisition, Review, and INW Server) to install the anti-virus software.
3. Configure the Computer Browser service. Refer to Configure Computer Browser Service Before Anti-Virus Installation for more information.
4. Configure the Remote Registry service. Refer to Configure Remote Registry Service Before Anti-Virus Installation for more information.

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

1. Click ***Start*** and launch ***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. 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. Click ***Add Client Install Feature Set…***. 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 ***14.2 RU1 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. Click ***Home*** in the ***Symantec Endpoint Protection Manager*** window.
13. Click ***Clients*** in the ***Symantec Endpoint Protection Manager*** window. Click ***Install a client*** under ***Tasks***. The ***Select Deployment Type*** screen displays.
14. Select ***New Package Deployment*** and click ***Next***. The ***Select Group and Install Feature Sets*** screen displays.
15. Select the following:
    - Install Packages: Windows – Symantec EndPoint Protection version 14.2.5569.2100-English.
    - Install Feature Sets: The feature sets name created in step 8.

    Keep the other settings as default and click ***Next***. The ***Symantec Endpoint Protection to Remote Computers*** screen displays.
16. Select ***Remote push*** and click ***Next***. Wait for the ***Computer selection*** screen to appear.
17. 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 ***Computer name or IP address*** detection method to identify the client systems (Acquisition, Review, and INW Server).

18. Select all Mac-Lab/CardioLab client machines connected to the domain and click **>>**. The ***Login Credentials*** screen displays.
19. Enter the user name, password and domain/computer name and click ***OK***.
20. Make sure all selected machines appear under ***Install Protection Client On*** and click ***Next***. The ***Install Symantec Endpoint Protection Client*** screen displays.

21. 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.

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

23. Wait until the Symantec icon displays in system tray and then restart all the client machines (Acquisition, Review, and INW Server). Log on as a user who is a member of the local\domain administrator 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 policy*** 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 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. 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. Click Exceptions from left pane.

71. Click the ***Add*** drop-down and select ***Windows Exceptions > Folder***.

72. Enter Mac-Lab/CardioLab folder paths one at a time and perform the following. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded:

    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. Click ***OK*** to add the exception.

73. Click ***OK***.

74. Click ***OK***.

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

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

77. Click ***Yes***.

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

79. Under ***My Company*** select ***Default Group*** and uncheck ***Inherit policies and settings from parent group "My Company"*** and click ***Communications*** 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.

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

81. Click ***OK***.

82. Click ***General*** settings under ***Location-independent Policies and Settings***.

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

84. Click ***OK***.

85. Click ***Admin*** and select ***Servers***.

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

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

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

89. Click ***OK***.

90. 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. Configure the Computer Browser service. Refer to Configure Computer Browser Service After Anti-Virus Installation for more information.
2. Configure the Remote Registry service. Refer to Configure Remote Registry Service After Anti-Virus Installation for more information.

McAfee VirusScan Enterprise (8.8 Patch 14)

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 a user who is a member of the local administrator.
2. Insert the **McAfee VirusScan Enterprise 8.8 Patch 14**, **CD** into the CD drive.
3. Double-click ***SetupVSE.Exe***. The Windows SmartScreen can’t be reached now dialog displays.
4. Click ***Run***. Click Yes on the UAC. 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 VirusScan 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*** and click ***Close***.
12. If a message box to restart the system displays, click ***OK***.
13. Restart the system.
14. Log on as a user who is a member of the local administrator.

McAfee VirusScan Enterprise Configuration

1. Click ***Start*** and launch ***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 ***On-Delivery Email Scanner*** and select ***Properties***. The ***On-Delivery Email Scan Properties*** screen appear.
6. 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***.
7. Uncheck ***Detect unwanted programs*** under ***Unwanted programs detection***.
8. Select ***Disabled*** for ***Sensitivity level*** under ***Artemis (Heuristic network check for suspicious files)***.
9. Click ***OK***.
10. 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 Mac-Lab/CardioLab folders one at a time and select ***OK***. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded.
27. Select ***Also exclude subfolders*** in the ***Add Exclusion Item*** window and click ***OK***.
28. Make sure Mac-Lab/CardioLab folders are present in Set Exclusions window. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded.

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 Mac-Lab/CardioLab folders one at a time and select ***OK***. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded.

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

45. Make sure Mac-Lab/CardioLab folders are present in the ***Set Exclusions*** window. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded.

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 (5.10.0)

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 14.

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 a user who is a member of the local\domain administrator group on all client systems (Acquisition, Review, and INW Server) to install the anti-virus software.

3. For New Installation, add the following agent version to the McAfee ePolicy Orchestrator master repository in McAfee ePolicy Orchestrator Console: ***- McAfee Agent v5.6.4.151.***

4. 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 14: VSE880LMLRP14.ZIP (v8.8.0.2190).

5. 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 14: VIRUSSCAN8800 v8.8.0.732 and VIRUSSCANREPORTS v1.2.0.452

NOTE: The VIRUSCAN8800(732).zip and VIRUSCANREPORTS120(452).zip can be found in McAfee VirusScan Enterprise 8.8 Patch 14 package.

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

1. Click ***Start*** and ***Launch McAfee ePolicy Orchestrator 5.10.0 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 username and password of user who is a member of the domain\local administrator 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 ***Target 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 5.6.4 (Current)***. Enter the username and password of user who is a member of the domain\local administrator 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 a user who is a member of domain\local administrator group.
12. Click ***Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.10.0 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 8.8.0.2190

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 user who is a member of the domain\local administrator group on all client machines.
27. Click the ***Log Off*** link to close the McAfee ePolicy Orchestrator Console.

McAfee ePolicy Orchestrator -Server Console Configuration

1. Depending on the software version, click ***Start*** and ***Launch McAfee ePolicy Orchestrator 5.10.0 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 Mac-Lab/CardioLab folders one at a time and select Also exclude subfolders. Click ***OK***. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded.
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 Mac-Lab/CardioLab folders one at a time and select ***Also exclude subfolders***. Click ***OK***. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded.

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 Mac-Lab/CardioLab folders one at a time and select ***Also exclude subfolders***. Click ***OK***. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded.

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 Mac-Lab/CardioLab folders one at a time and select ***Also exclude subfolders***. Click ***OK***. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded.

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 Mac-Lab/CardioLab folders one at a time and select ***Also exclude subfolders***. Click ***OK***. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded

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 Mac-Lab/CardioLab folders one at a time and select ***Also exclude subfolders***. Click ***OK***. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded.

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\GE Healthcare\MLCL\**, **C:\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.

Trend Micro OfficeScan Client/Server Edition (XG SP1)

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 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

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 a user who is a member of the domain\local administrator group on all client systems (Acquisition, Review, and INW Server) to install the anti-virus software.
4. Configure the Computer Browser service. Refer to Configure Computer Browser Service Before Anti-Virus Installation for more information.
5. Configure the Remote Registry service. Refer to Configure Remote Registry Service Before Anti-Virus Installation for more information.

Trend Micro OfficeScan - New Installation Deployment Steps (Preferred Push Installation Method for XG 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 ***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 a user who is a member of the domain\local administrator 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

1. Select ***Start*** and launch ***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 Mac-Lab/CardioLab folders one at a time click **+**. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded.

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 Mac-Lab/CardioLab folder paths are present in the ***Exclusion List***. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded.

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 Mac-Lab/CardioLab folder paths are present in the Exclusion List. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded.

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 Mac-Lab/CardioLab folder paths are present in the Exclusion List. Refer to the Mac-Lab/CardioLab Folders Exclusion for the folders to be excluded.

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

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

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

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

    - ***Scan > Configure Manual Scan Settings.***
    - ***Scan > Configure Real-time Scan Settings.***
    - ***Scan > Configure Scheduled Scan Settings.***
    - ***Proxy Setting Privileges > Allow users 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.

60. Click the ***Other Settings*** tab.

61. 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.***

62. Click ***Apply to All Agents***.

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

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

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

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

67. Uncheck all options.

68. Click ***Apply to All Agents***.

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

70. From the top pane, select the ***Agents > Global Agent Settings*** link.

71. 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.***

72. Click ***Save***.

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

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

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

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

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

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

Trend Micro OfficeScan Post Installation Guidelines

1. Configure the Computer Browser service. Refer to Configure Computer Browser Service After Anti-Virus Installation for more information.
2. Configure the Remote Registry service. Refer to Configure Remote Registry Service After Anti-Virus Installation for more information.

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

During the preferred push installation methods for Trend Micro OfficeScan Client/Server Edition XG SP1, 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 XG SP1, see Trend Micro OfficeScan - New Installation Deployment Steps (Preferred Push Installation Method for XG SP1) on page 26.

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. 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 a user who is a member of the domain\local administrator 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 credentials of user who is a member of the domain\local administrator group.

   d. Navigate to **\\<*Anti-Virus Management Console_server_IP _address*>\ofsscan** and double-click ***AutoPcc.exe***. When prompted enter the credentials of user who is a member of the domain\local administrator group.

   e. If prescan is configured, wait for the prescan to complete before the installation begins.

   f. Restart the client systems when the installation is complete.

   g. Log in as a user who is a member of the domain\local group on all client machines and wait until the Trend Micro OfficeScan icon in system tray changes to blue.

   h. For XG SP1, see Trend Micro OfficeScan Server Console Configuration for XG SP1 on page 27.

Anti-virus Software Port and Firewall Exceptions

Note: Refer to your anti-virus software documentation for required port and process exceptions. Below is the minimal configuration determined by testing. These port and process exceptions must be configured.

Symantec Endpoint Protection

Process Exceptions:

- Symantec Endpoint Protection Manager
- Symantec Endpoint Protection Manager Webserver

McAfee Virus Scan Enterprise

Process Exceptions:

- macmnsvc

McAfee ePolicy Orchestrator

Process Exceptions:

- McAfee ePolicy Orchestrator 5.10.0 Application Server
- McAfee ePolicy Orchestrator 5.10.0 Event Parser
- McAfee ePolicy Orchestrator 5.10.0 Server

Trend Micro Office Scan

Port Exceptions:

- TCP 4343 (Trend Micro OfficeScan Server HTTPS)
- TCP 8080 (Trend Micro OfficeScan Server HTTP)
- TCP <listener port> (Trend Miro OfficeScan Listner)