Mac-Lab/CardioLab Anti-Virus Information
Software version 6.9.6

Product Group: Interventional Invasive Products

Products:
Mac-Lab IT/XT/XTi, CardioLab IT/XT/XTi,
SpecialsLab and ComboLab IT/XT/XTi
Recording Systems, Centricity Cardiology
Data Management Systems

Subject: Anti-Virus Information

Date: 25-February-2015
Mac-Lab/CardoLab/INW Server v6.9.6 Anti-Virus Installation

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

Anti-Virus Requirements

WARNING:

ANTI-VIRUS SOFTWARE INSTALLATION

The System is delivered without anti-virus protection. It is recommended to have validated anti-virus software 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 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 version 6.9.6 systems have been validated to run with the software listed in the following table.

<table>
<thead>
<tr>
<th>Supported Anti-Virus Software</th>
<th>Supported Languages</th>
<th>Supported Anti-Virus Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee VirusScan Enterprise</td>
<td>English</td>
<td>8.8 Patch 3</td>
</tr>
<tr>
<td>McAfee ePolicy Orchestrator (with McAfee VirusScan Enterprise 8.8 Patch 3)</td>
<td>English</td>
<td>v5.0</td>
</tr>
<tr>
<td>Symantec EndPoint Protection</td>
<td>English</td>
<td>12.1.2</td>
</tr>
<tr>
<td>Trend Micro OfficeScan Client/Server Edition</td>
<td>English</td>
<td>10.6 SP2</td>
</tr>
</tbody>
</table>

**NOTE:** Previously supported CA Total Defense Anti-Virus is no longer a commercially available product.

**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 as a result of following the procedures in this manual, elevate with the same administrator or member of that group account that you have logged in as.

**Customer-Provided Server Configuration**

The anti-virus management console is required to be installed on the Customer-Provided Server.

The communication between Customer-Provided Server and Mac-Lab/CardioLab devices can be accomplished in different ways including:

1. Adding to INW domain.
2. Adding to Member Server domain.
3. Cross domain authentication.
   
   **NOTE:** The customer-provided 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.

**Anti-Virus Installation Instructions**

**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. Click **Turn on file and printer sharing**.
5. Click **Save changes**.
6. Click **Start > Run**.
7. Type `services.msc` and press **Enter**.
8. Double-click the **Computer Browser** service.
9. Change the **Startup type** to **Automatic**.
10. Click **Start**.
11. Click **OK**.
12. Close the **Services** window.

**Configure Computer Browser Service After 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 > 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

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 customer-provided 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 for English.

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. On the customer-provided server, make sure Symantec EndPoint Protection Manager is installed before continuing with these steps.
2. On the customer-provided server, open inbound port 8014 and name it IN_8014_Symantec and allow inbound connections for domain, public, and private.
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.

Symantec EndPoint Protection Deployment Steps (Preferred Push Installation Method)

1. Click Start > All Programs > Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager.
2. Enter the appropriate 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.
4. Click Home in the Symantec Endpoint Protection Manager window.
5. Select Install protection client to computers from the Common Tasks drop-down list in the top-right of the Home window.
7. Keep the default settings and click Next.
9. 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).

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

11. Enter the appropriate user name, password and domain name and click OK.

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

13. 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 appears.

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

15. 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 appropriate Symantec Endpoint Protection Manager Console password and click Log On.


4. Click Add a Virus and Spyware Protection policy under Tasks. The Virus and Spyware Protection window opens.


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 Notification about detections when the user logs on.

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


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, uncheck and lock the When Auto-Protect is disabled, Enable after: option.


23. Uncheck Rescan cache when new definitions load and click OK.


25. Select the Notifications tab and uncheck and lock Display a notification message on the infected computer.

26. Under Windows Settings > Email Scans, click Internet Email Auto-Protect.

27. 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.

28. Under Windows Settings > Email Scans, click Microsoft Outlook Auto-Protect.

29. Select the Notifications tab and uncheck and lock Display a notification message on the infected computer.

30. Under Windows Settings > Email Scans, click Lotus Notes Auto-Protect.

31. Select the Notifications tab and uncheck and lock Display a notification message on infected computer.

32. Under Windows Settings > Advanced Options, click Quarantine.

33. Under When New Virus Definitions Arrive, select Do nothing.

34. Under Windows Settings > Advanced Options, click Miscellaneous.

35. 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.

36. Click OK to close Virus and Spyware Protection policy.

37. Click Yes at the Assign Policies message box.

38. Select My Company and click Assign.
39. Click Yes at the message box.
40. Under Policies click LiveUpdate.
41. Select LiveUpdate Settings policy and under Tasks, click Edit the policy.
42. Under Overview > Windows Settings, click Server Settings.
43. Under Internal or External LiveUpdate Server, ensure Use the default management server is selected and uncheck Use a LiveUpdate server.
44. Click OK.
45. Click Clients from left pane and select the Policies tab.
46. Uncheck Inherit policies and settings from parent group "My Company" and click Communications Settings under Location-Independent Policies and Settings.
47. Under Download, make sure Download policies and content from the management server is checked and Push mode is selected.
48. Click OK.
49. Click General Settings under Location-independent Policies and Settings.
50. Select the Tamper Protection tab and uncheck and lock Protect Symantec security software from being tampered with or shut down.
51. Click OK.
52. Click Admin and select Servers.
53. Under Servers, select Local Site (My Site).
54. Under Tasks, select Edit Site Properties. The Site Properties for Locate Site (My Site) window opens.
55. Select LiveUpdate tab and under Download Schedule ensure the schedule is set to Every 4 hour(s).
56. Click OK.
57. Click Policies and select Firewall.
58. Select Firewall policy and under Tasks click Edit the policy. The Firewall policy window opens.
59. Click Protection and Stealth and under Protection Settings uncheck Automatically block an attacker's IP address.
60. Click OK.
61. 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.
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 for English.

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 the McAfee VirusScan Enterprise 8.8 Patch 3 CD into the CD drive.
4. Click Yes. The McAfee VirusScan Enterprise Setup screen appears.
5. Click Next. The McAfee End User License Agreement screen appears.
6. Read the license agreement and complete any necessary fields, click OK when finished.
7. Select Typical and click Next.
8. Select Standard Protection and click Next.
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 appears.
10. Uncheck the Run On-Demand Scan checkbox and click Finish.
11. If the Update in Progress window appears, click Cancel.
12. If a message box to restart the system appears, click OK.
13. Restart the system.
14. Log on as Administrator or as a member of that group.

McAfee VirusScan Enterprise Configuration

1. Right-click McAfee in the system tray and select On-Access Scan Properties.
2. Select the ScriptScan tab. The ScriptScan window opens.
3. Clear the Enable scanning of scripts check box.
5. Uncheck the Show the messages dialog when a threat is detected and display the specified text in the message check box.
6. Click Apply.
7. Click OK to close the On-Access Scan Properties window.
8. Select Start > All Programs > McAfee > VirusScan Console. The VirusScan Console window opens.
10. Uncheck the On-Access Scan, On-Demand Scan and scheduled scans, Email Scan and AutoUpdate check boxes.
11. Click Destination. The Alert Manager Client Configuration window opens.
12. Select the Disable alerting check box.
13. Click OK. The Alert Properties window opens.
14. Select the Additional Alerting Options tab.
15. Select the Suppress all alerts (severities 0 to 4) option from the Severity Filter drop-down list.
16. Select the Alert Manager Alerts tab.
17. Clear the Access Protection check box.
18. Click Apply.
19. Click OK to close the Alert Properties window.
20. Right-click AutoUpdate on the VirusScan Console.
22. Click Schedule. The Schedule Settings window opens.
23. Clear the Enable (scheduled task runs at specified time) check box.
24. Click Apply.
25. Click OK to close the Schedule Settings window.
26. Click OK to close the McAfee AutoUpdate Properties – AutoUpdate window.
27. Right-click Full Scan on the VirusScan Console.
28. Click Properties. The On Demand Scan Properties window opens.
29. Click Schedule. The Schedule Settings window opens.
30. Check the Enable (scheduled task runs at specified time) check box.
31. Select the Schedule tab.
32. Select Weekly from Run Task, 12:00 AM from Start Time. check Sunday from Schedule Task Weekly.
33. Click OK. The On Demand Scan Properties - Full Scan window opens.
34. Select the Exclusions tab.
35. Click Exclusions. The Set Exclusions window opens.
36. Click **Add**.

37. Click **Browse** and navigate to `C:\Program Files\GE Healthcare\MLCL` and `D:\GEData\Studies\` folders one at a time and select the **Also exclude subfolders** checkbox.

38. Click **OK**.

39. In the **Set Exclusions** window, make sure the `C:\Program Files\GE Healthcare\MLCL` and `D:\GEData\Studies\` folders display.

40. Click **OK**.

41. Click **OK** to close the **On Demand Scan Properties – Full Scan** window.

42. Close the **VirusScan Console**.
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 customer-provided 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 for English.

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. Make sure McAfee ePolicy Orchestrator Console is installed on the customer provided server before continuing with these steps.
2. On the customer-provided server, open inbound port 443 and name it IN_443_McAfee and allow inbound connections for domain, public, and private.
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.

McAfee ePolicy Orchestrator Deployment Steps (Preferred Push Installation Method)

1. Select Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console to log on to the ePolicy Orchestrator console.
   NOTE: Click Continue with this website if the Security Alert message box appears.
2. Enter the appropriate username and password and click Log On.
3. Select Menu > Configuration > Server Settings > Port.
4. Record the Agent-to-server communication port number.
5. On the customer-provided server, open the Agent-to-server communication port as an inbound port and name it IN_<port number>_McAfee.
6. Select Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console to log on to the ePolicy Orchestrator console.
   NOTE: Click Continue with this website if the Security Alert message box appears.
7. Enter the appropriate username and password and click Log On.
9. Click My Organization and with the focus on My Organization click System Tree Actions > New Systems from the bottom left corner of the screen.
10. Select *Push agents and add systems to the current group (My Organization)* and click *Browse*.

11. Enter the *domain administrator* username and password and click *OK*.

12. Select the *INW* domain from the *Domain* drop-down list.

13. Select the client machines (Acquisition, Review, and INW Server) connected to the domain and click *OK*.

14. Select *Agent Version* as *McAfee Agent for Windows 4.8.0 (Current)*. Enter appropriate domain administrator username and password and click *OK*.

15. In client machines (Acquisition, Review, and INW Server) make sure the `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.

16. Restart the client machines (Acquisition, Review, and INW Server).

17. Click *Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console*.

18. Enter the appropriate username and password and click *Log On*.

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

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

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

22. Select the following:
    
    a. *Product*: McAfee Agent
    b. *Task Type*: Product Deployment
    c. *Task name*: Create New Task

23. 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
    d. *Options*: Run at every policy enforcement (Windows only)

24. Click *Save*.

25. 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

26. Click **Next.** The **2 Schedule** screen appears.

27. Select **Run immediately** from **Schedule type** drop-down list.

28. Click **Next.** The **3 Summary** screen appears.

29. Click **Save.** The **System Tree** screen appears.

30. Select the **Systems** tab and then select all the client machines (Acquisition, Review, and INW Server) which are connected to the domain.

31. Click **Wake up Agents** at bottom of the window.

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

33. 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.

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

**McAfee ePolicy Orchestrator Server Console Configuration**

1. Select **Start > All Programs > McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console** to log on to the ePolicy Orchestrator console.

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

2. Enter the appropriate Username and Password. The **ePO Summary** window opens.

3. Select **Menu > Systems > Systems Tree.** The **System Tree** window opens.

4. Click **My Organization.**

5. Select the **Assigned Policies** tab. The **Assigned Policies** screen opens.

6. From the **Product** drop-down list, select **VirusScan Enterprise 8.8.0**. The **Assigned Policies** window for VirusScan Enterprise 8.8.0 opens.

7. Click **My Default** for **On-Access General Policies.** The **General** window opens.

8. Select **Workstation** from the **Settings for** drop-down list. Click **ScriptScan** and uncheck **Enable scanning of scripts.**

9. Click **Messages.** The **Messages** window opens.

10. Uncheck **Show the messages dialog box when a threat is detected and display the specified text in the message.**

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

12. Click **ScriptScan** and ensure **Enable scanning of scripts** is unchecked.

13. Click **Messages.** The **Messages** window opens.
14. Uncheck the *Show the messages dialog box when a threat is detected and display the specified text in the message*.

15. Click *Save*.


17. Select *Workstation* from the *Settings for* drop-down list and uncheck *Show the messages dialog box when a buffer overflow is detected*.

18. Select *Server* from the *Settings for* drop-down list and uncheck *Show the messages dialog box when a buffer overflow is detected*.

19. Click *Save*.


21. Select *Workstation* from the *Settings for* drop-down list and uncheck *On-Access Scan, On-Demand Scan and scheduled scans, Email Scan and AutoUpdate*.

22. Check *Disable alerting*.

23. Click *Additional Alerting Options*. The *Additional Alerting Options* window opens.

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

25. Select *Server* from the *Settings for* drop-down list and select the *Alert Manager Alerts* tab. The *Alert Manager Alerts* window opens.

26. Uncheck *On-Access Scan, On-Demand Scan and scheduled scans, Email Scan and AutoUpdate*.

27. Check *Disable alerting*.

28. Click *Additional Alerting Options*. The *Additional Alerting Options* window opens.

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

30. Click *Save*.


32. Select *Workstation* from the *Settings for* drop-down list and ensure *Configure one scanning policy for all processes* is selected.

33. Click the *Exclusions* tab. The *Exclusions* window opens.

34. Click *Add* and select *By pattern*.

35. Enter the C:\Program Files\GE Healthcare\MLCL and D:\GEData\Studies folder names and select *Also exclude subfolders*.

36. Click *OK*.

37. Select *Server* from *Settings for* drop-down list and select the *Processes* tab.

38. Ensure *Configure one scanning policy for all processes* is selected.
39. Select the **Exclusions** tab. The **Exclusions** window opens.
40. Click **Add** and select **By pattern**.
41. Enter `C:\Program Files (x86)\GE Healthcare\MLCL` and select **Also exclude subfolders**.
42. Click **OK**.
43. Click **Save**.
44. From the **Product** drop-down menu, select **McAfee Agent**. The **Policies** window for McAfee Agent opens.
45. Click **My Default** for **Repository**. The **Repositories** window opens.
   **NOTE:** Click **Close** for **Internet Explorer Security Message Box**.
46. Click **Proxy**. The **Proxy** window opens.
47. Select **Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)**.
48. Click **Save**.
49. Click **Systems**.
50. Select all the client systems (Acquisition, Review and Centricity Cardiology INW server) into which the configured policies are to be deployed.
51. Select **Wake Up Agents**. The **Wake Up Agent** window opens.
52. Click **OK**.
53. Log off ePolicy Orchestrator.

**McAfee ePolicy Orchestrator Post Installation**

Enable the Loopback Connection. Refer to Enable Loopback Connection on page 6 for more information.
Trend Micro OfficeScan Client/Server Edition

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 customer-provided 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 for English.

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. On the customer-provided server, make sure Office Scan Web Console is installed before continuing with these steps.
2. On the customer-provided server, open inbound port 8080 and name it IN_8080_OSCE and allow inbound connections for domain, public, and private.
3. Log on as Administrator or 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.

Trend Micro OfficeScan 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.
4. Click Install.
5. Enter appropriate 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.
10. Click **Install**.

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

12. Expand the appropriate 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. Click **Start > Run**.
   
b. Enter `\<customer_provided_server_IP_address>` and press Enter.
   
c. Navigate to `\<customer_provided_server_IP_address>\ofsscan` and double-click **AutoPcc.exe**.
   
d. Restart the client systems when the installation is complete.
   
e. 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.
   
f. Click the **Log Off** link to close the **OfficeScan Web Console**.
   
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. Enter the appropriate `<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 sin wave 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** window appears.

2. Enter the appropriate user name and password and click **Login**. The **Summary** window opens.

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 **Privileges and Other Settings**.
6. Select only the following options in the **Privileges** tab and clear 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.
   - Unloading > Require a password for the user to unload the OfficeScan client. Enter a suitable password.

7. Select the **Other Settings** tab.

8. Select **Client Security Settings > Normal** and clear the remaining options.

9. Click **Apply to All Clients**.

10. Click **Close** to close the **Privileges and Other Settings** window.

11. From the left side pane, select the **Client Management** link.

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

13. From the **Settings** options, select **Scan Settings > Scan Now Settings**.

14. Select only the following options in the **Target** tab and clear 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 and D:\GEData\Studies folders one at a time in the directory path for Exclusion List and click **Add**.

15. Click **Apply to All Clients**.

16. 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 will appear. Click **OK**.

17. Click **Close** to close the **Scan Now Settings** page.

18. From the left side pane, select the **Client Management** link.

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

20. From the **Settings** options, select **Settings->Scan Settings->Real-time Scan Settings**.

21. Select the **Target** tab. Select only the following options and clear the remaining options:
   - Enable Virus/Malware scan.
22. Click the **Action** tab.

23. Keep the default settings and clear **Virus/Malware > Display a notification message on the client computer when Virus/Malware is detected** option and **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 **Real-time Scan Settings** page.

26. From the left side pane, select the **Client Management** link.

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

28. From the **Settings** options, select **Scan settings > Scheduled Scan Settings**.

29. Select the **Target** tab. Select only the following options and clear the remaining options:
   - **Enable Virus/Malware scan**.
   - **Schedule > Weekly, every (Sunday)**.
   - **Files to Scan > File types scanned by IntelliScan**.
   - **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 and D:\GEData\Studies paths are present in the **Exclusion List**.

30. Click the **Action** tab.

31. Keep the default settings and uncheck the **Virus/Malware > Display a notification message on the client computer when Virus/Malware is detected** and **Spyware/Grayware > Display a notification message on the client computer when spyware/Grayware is detected** options.

32. Click **Apply to All Clients**.

33. Click **Close** to close the **Scheduled Scan Settings** page.

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

35. Select only the following options and clear 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.

36. Click **Save**.

37. 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.