


**Artwork and Signature File for:
MAN-00525, "MIMsv1.0 Antivirus FMI"**

Artwork consists of:

- Eight (8) 8 ½ inch x 11 inch pages.

REV AUTHORED BY R. SEBASTIAN	DATE 10/18/07	 HOLOGIC [®] A FAMILY OF COMPANIES	Osteoporosis Assessment LORAD [®] Breast Cancer Detection DirectRay [®] Digital Imaging FLUOROSCAN [®] C-arm Imaging		SIGNATURES ON FILE
REV DRAFTED BY R. SEBASTIAN	DATE 10/18/07		TITLE MIMsv1.0 Antivirus Validation Protocol	DOCUMENT NUMBER AW-01350	
PROPRIETARY: This document contains proprietary data of Hologic, Inc. No disclosure, reproduction or use of any part thereof may be made except by written permission from Hologic.		ARTWORK	SIZE A	SHEET 1 OF 1	
REV. RELEASE DATE:	10/24/07				

MIMS v.1.0 Anti-virus installation instructions

Purpose:

To install anti-virus software on the Mammography Image Management Solutions (MIMS), Hologic's departmental image archive and connectivity product.

Scope:

This document applies only to MIMS model MIMS v1.0. MIMS v1.0 is loaded with Impax 4.1 application software which runs over Windows 2000 Server, utilizing a Dell PowerEdge 2600 server as it's hardware platform. Note: the MIMS v1.0 model was originally marketed as "MIMS." The "v1.0" was added to distinguish it from other MIMS configurations as noted below. Check the Hologic web site (<http://www.hologic.com/cc/network>) for other documents, which cover anti-virus installation instructions on the following MIMS models:

- **MIMS v1.1** Impax 5.2 application software which runs over Windows 2003 Server, utilizing a Dell PowerEdge 2600 server as it's hardware platform.
- **MIMS v1.2** Impax 5.2 application software which runs over Windows 2003 Server, utilizing a Dell PowerEdge 2800 server as it's hardware platform.

Estimated Time:

Installation of anti-virus products will take a computer technician approximately 30 minutes to complete. This includes running live-update and verifying auto-protect is enabled.

Reference List

Table 1: Reference List

Name	Comments
Symantec AntiVirus Corporate Edition 10.0	Customer provided. Only the client component of the Corporate edition can be loaded on this product.
McAfee 8.0i Antivirus	Customer provided. Only the client component can be loaded on this product.
McAfee 8.5i Antivirus	Customer provided. Only the client component can be loaded on this product.

Definitions

Liveupdate – A feature that allows servers and clients to retrieve updates from an internal server or Symantec's official Live Update server.

Managed – The client system is configured to send virus alerts, as well as retrieve virus updates, from an internal parent Symantec server.

Real-time– Real time scanning of each file that is loaded in RAM. Real-time protection can be used with Smartscan.

Smartscan – A scanning technique that scans the header of each file to determine its true file extension and

to identify possible malicious code.

Unmanaged – The clients do not connect to the network nor do they have a parent server with which they communicate with. System administrators must manually download virus definition updates for unmanaged clients.

1.0 Customer Preparation Checklist

Prior to beginning the installation, the following must be arranged with the customer:

- Make sure that the customer has purchased and procured the anti-virus software. Hologic does not supply the customer with this software. It is the customer's responsibility to purchase the software and associated licenses.
- Customers must provide their own Symantec Server within their networked environment. Only client software should be loaded on the MIMS products. The clients will retrieve updates from their existing Symantec Server, should they choose to install the client software in a "managed" state. For customers who want their installations to interface with their existing Symantec server, choose "Managed" setup. Customers who cannot provide their own Symantec Server must set the anti-virus software to obtain updates directly from Symantec.

2.0 Pre-installation Checklist

Prior to beginning the installation, review the following:

- Ensure that no existing anti-virus software is loaded on the MIMS prior to installation.
- Ensure that the installer has proper serial keys and associated licenses for the product that is to be installed.
- Ensure that the installer is logged into the MIMS as an administrator and the Impax software is stopped.
- Ensure that at least 390mb of disk drive space is available on the C: drive before antivirus installation (Reference MAN-00524, section 6.8 for disk drive configurations)

3.0 Installing Symantec AntiVirus 10.0 as an unmanaged client



Note Autoplay should bring up the Symantec menu. If it does not, browse to the D: drive and launch the executable from that location.

1. On the MIMS, login to Windows as an Administrator.

2. Installation procedures:

- a. Insert the "Symantec AntiVirus 10.0" cd from the Symantec AntiVirus package.
- b. Autoplay should bring up the menu. If it does not, browse to the D: drive and launch the setup icon.
- c. When the window appears, click "**Install Symantec AntiVirus.**"
- d. A second window will appear. Again, select "**Install Symantec AntiVirus.**"
- e. When the "**Welcome to the InstallShield Wizard for Symantec AntiVirus**" appears, click **NEXT**.
- f. Click "**I accept the terms in the license agreement.**"
- g. A window will appear prompting the user for 2 options. Client install and Server install.
- h. Select "**Client install**" and proceed to the next window.
- i. Click the "**Complete**" checkbox and click next.
- j. Select "**Unmanaged**" and click next.
- k. Ensure Auto-Protect and Run-LiveUpdate are checked and proceed to the next section by clicking "**Next.**"
- l. Click the "**Install**" button.
- m. After the installation completes, click "**Finish.**"
- n. Reboot the MIMS.

3. Configuring Symantec AntiVirus 10.0

- a. After the MIMS boots back into windows, log back in as an **Administrator**.
- b. You should be presented with a window that states, "**License not found.**"
- c. Click the hyperlink <http://licensing.symantec.com/>
- d. Enter your serial number and click **NEXT**. You should receive an .sfl file via email. If you do not, contact Symantec Technical Support.
- e. Copy the **.sfl file** over to the C: drive
- f. Locate the **auto-protect shield** at the bottom right of your screen.
- g. Right click the icon and select "**Open Symantec AntiVirus.**"
- h. When the console appears, expand "**View.**" Double click "**License.**"
- i. In the right pane of the console window, click "**Install license.**"
- j. Select "BROWSE" and locate the .sfl you placed on your C: drive.
- k. Click "**Next.**"
- l. Close the Symantec AntiVirus console.

4. Configuring Real-time Protection (Autoprotect)

- a. Open up the virus scan console
- b. From the top of the window, choose Configure > File System Real-time Protection
- c. Click the hyperlink Locate "File Types." Change this setting to "**Selected.**"
- d. Click "Exclude selected files and folders" and click the **Exclusions** tab
- e. Click "Check file for exclusion before scanning."
- f. Click "Files or Folders."
- g. Ensure you place a "check" on the following boxes, so that the respective drives will be properly

excluded from real-time scanning:

- Database (E:)
- Volumes (F)
- Logs (G:)
- Cache (H:)



Note "Selected" scanning with smartscan scans the header of each file to determine the file type. By default, it will scan 57 extensions and it is fully configurable. To scan all files entering and leaving the MIMS, leave "All files" checked. This may degrade performance on your MIMS.



Note "The A:, C: and D: drives should NOT be checked under Files and Folders exclusions.

4.0 Installing Symantec AntiVirus 10.0 as a managed client



Note Autoplay should bring up the Symantec menu. If it does not, browse to the D: drive and launch the executable from that location.

1. On the MIMS, login to Windows as an Administrator.

2. Installation procedures:

- Insert the "Symantec AntiVirus 10.0" cd from the Symantec AntiVirus package.
- Autoplay should bring up the menu. If it does not, browse to the D: drive and launch the setup icon.
- When the window appears, click "**Install Symantec AntiVirus.**"
- A second window will appear. Again, select "**Install Symantec AntiVirus.**"
- When the "**Welcome to the InstallShield Wizard for Symantec AntiVirus**" appears, click **NEXT**.
- Click "**I accept the terms in the license agreement.**"
- A window will appear prompting the user for 2 options. Client install and Server install.
- Select "**Client install**" and proceed to the next window.
- Click the "**Complete**" checkbox and click next.
- Select "**Managed**" and click next.
- At the next screen, click the **BROWSE** button and locate your Symantec Server
- Click the "**Install**" button.
- Click **NEXT**.
- Ensure autoprotect and liveupdate are checked and click **NEXT**

3. Configuring Symantec AntiVirus 10.0

- After the MIMS boots back into windows, log back in as an **Administrator**.
- You should be presented with a window that states, "**License not found.**"
- Click the hyperlink <http://licensing.symantec.com/>
- Enter your serial number and click **NEXT**. You should receive an .sfl file via email. If you do not, contact Symantec Technical Support.
- Copy the **.sfl file** over to the C: drive

- f. Locate the **auto-protect shield** at the bottom right of your screen.
- g. Right click the icon and select **“Open Symantec AntiVirus.”**
- h. When the console appears, expand **“View.”** Double click **“License.”**
- i. In the right pane of the console window, click **“Install license.”**
- j. Select **“BROWSE”** and locate the .sfl you placed on your C: drive.
- k. Click **“Next.”**
- l. Close the Symantec AntiVirus console.

5. Configuring Real-time Protection (Autoprotect)

- a. Open up the virus scan console
- b. From the top of the window, choose Configure > File System Real-time Protection
- c. Click the hyperlink Locate **“File Types.”** Change this setting to **“Selected.”**
- d. Click **“Exclude selected files and folders”** and click the **Exclusions** tab
- e. Click **“Check file for exclusion before scanning.”**
- f. Click **“Files or Folders.”**
- g. Ensure you place a **“check”** on the following boxes, so that the respective drives will be properly excluded from real-time scanning:
 - Database (E:)
 - Volumes (F)
 - Logs (G:)
 - Cache (H:)



Note **“Selected” scanning with smartscan scans the header of each file to determine the file type. By default, it will scan 57 extensions and it is fully configurable. To scan all files entering and leaving the MIMS, leave “All files” checked. This may degrade performance on your MIMS.**



Note **“The A:, C: and D: drives should NOT be checked under Files and Folders exclusions.”**

5.0 Installing McAfee 8.0i

- 1. On the MIMS, login to Windows as Administrator.**
- 2. Installation procedures:**
 - a. Insert the "McAfee 8.0i cd."
 - b. Autoplay should bring up the menu. If it does not, browse to the D: drive and launch the setup icon from there.
 - c. The McAfee console should appear
 - d. Click "**VirusScan v8.0i for Win NT/2k/XP**"
 - e. Click "Install VirusScan v8.0i"
 - f. Click "**Next.**"
 - g. Choose the appropriate licensing information, click "I accept" and click "OK."
 - h. Choose "Typical" installation and click "Next." Now click "Install."
 - i. When installation is complete, unselect Update Now and Run On-Demand Scan
 - j. Click "**Finish.**" You may be prompted to reboot.
 - k. Reboot the system
- 3. Configuring McAfee 8.0i**
 - a. After the MIMS boots back into windows, log back in as "**Administrator.**"
 - b. Double click the McAfee shield in the system tray and choose "Properties."
 - c. On the left window, click "All Processes."
 - d. Click the "Detection" tab at the top. Select "On Network Drives."
 - e. Now click the "Advanced" tab at the top.
 - f. Under compressed files, select "Scan inside archives" and select "Decode MIME encoded files." Click "Apply" and exit the console.

6.0 Installing McAfee 8.5i

- 1. On the MIMS, login to Windows as Administrator.**
- 2. Installation procedures:**
 - a. Insert the "McAfee 8.5i cd."
 - b. Click NEXT to begin installation
 - c. Click I accept the terms in the license agreement
 - d. Choose TYPICAL install and click NEXT
 - e. Choose Standard Protection
 - f. Select install
 - g. When it is complete, uncheck "RUN ON DEMAND SCAN" and select FINISH. Or if you would like to scan your system now (off peak hours only) select "RUN ON DEMAND SCAN"
 - h. Click "**Finish.**" You may be prompted to reboot.
 - i. Reboot the system
- 3. Configuring McAfee 8.0i**
 - a. Launch the McAfee console
 - b. Ensure Access Protection is enabled
 - c. Ensure Buffer Overflow Protection is enabled
 - d. Ensure the On-Access Scanner is enabled
 - e. Double click ACCESS PROTECTION

- f. A new window should appear
- g. Ensure "prevent McAfee services from being stopped" is checked
- h. Now it's time to configure ANTIVIRUS STANDARD PROTECTION.
- i. Prevent registry editor and task manager from being disabled
- j. Prevent user rights policies from being altered
- k. Prevent remote creation of autorun files
- l. Prevent hijacking of .EXE and other executable extensions
- m. Prevent Windows Process spoofing
- n. Prevent mass mailing worms from sending mail
- o. Prevent IRC communication
- p. Prevent use of tftp.exe
- q. Now it's time to configure ANTIVIRUS MAXIMUM PROTECTION
- r. Prevent svchost executing non-Windows executables
- s. Protect cached files from password and email address stealers
- t. Now it's time to configure COMMON STANDARD PROTECTION
- u. Prevent modification of mcafee files and settings
- v. Prevent common programs from running files from the Temp folder
- w. Prevent termination of mcafee processes
- x. Prevent modification of mcafee common management (REPORT ONLY)
- y. Prevent modification of McAfee Scan Engine files (REPORT ONLY)
- z. Now it's time to configure COMMON MAXIMUM PROTECTION
- aa. Prevent programs registering to autorun (report only)
- bb. Prevent programs registering as a service (report only)
- cc. Prevent creation of new exe files in the windows folder (REPORT ONLY)
- dd. Prevent creation of new exe files in the program files (REPORT ONLY)

7.0 Manually installing updates

Symantec and Norton

1. **Downloading virus definitions when the MIMS does not have internet access.**
 - a. Use a PC with internet access and browse to <http://securityresponse.symantec.com/avcenter/download.html>
 - b. Download the proper virus definitions to the desktop
 - c. When the download completes, burn the executable to a CD.
2. **Manually installing the updates**
 - a. On the MIMS, login to Windows as **Administrator**.
 - b. Insert the media with the virus definitions
 - c. **Browse to D:** and double click the executable.
 - d. A window will appear and ask, "**Do you want to update your virus definition files?**"
 - e. Click "**yes.**"
 - f. After installation is complete, you will be presented with a window.
 - g. Read the contents of the message and press "**OK.**"
 - h. Reboot the MIMS if you are prompted.



Note "Unmanaged clients" must obtain their virus definition updates from Symantec.



Note "The above process may differ slightly for each Symantec product."

8.0 Manually installing updates

McAfee

3. Downloading virus definitions when the MIMS does not have internet access.

- a. Use a PC with internet access and browse to <http://www.mcafee.com/us/downloads/updates/dat.asp?id=1>
- b. Click "I agree"
- c. Locate and download the appropriate DAT files.
- d. When the download completes, burn the zip or executable to a CD.

4. Manually installing the updates

- a. On the MIMS, login to Windows as **Administrator**.
- b. Insert the media with the virus definitions
- c. **Browse to D:** and double click the executable.
- d. A window will appear, click "Next."

When it is finished, click "FINISH."

9.0 Verifying Installation

1. Verifying Anti-virus functionality

- a. Double click the Shield Icon in the taskbar
- b. Click "Liveupdate" and verify that the anti-virus software can communicate to the relevant server
- c. Reboot the MIMS and ensure that Auto-Protect starts upon logging in to Windows

2. Verifying MIMS functionality.

- a. Ensure that the Impax software starts correctly
- b. From a SecurView, perform a Query/Retrieve.
- c. Ensure the images can be retrieved correctly.

10.0 Scanning intervals

1. When to perform manual or automated scans

- a. Manual or automated scans should be set to scan ALL system and logical drives. This includes A:, C: D: E: F: G: and H: drives.
- b. The scan should be performed during non-peak hours (ie: When the system is in an idle state)