

1. Introduction

Antivirus software is an effective way to combat computer viruses, trojans, worms, and other malicious software that may attempt to compromise the integrity of a system. It is essential that antivirus software is installed and configured correctly and kept up to date for it to be an effective tool. Hologic has tested SecurView with the antivirus products in the reference list for the benefit of our customers.

1.1. Purpose

To install antivirus software on SecurView Workstation 7.x products.

1.2. Scope

This document applies to all SecurView products with version 7-0-x and 7.1.x software.

1.3. Estimated Time

Installation of antivirus products takes the network technician approximately 30 minutes to complete, including configuration.

1.4. Reference List

This document provides instructions for the following products.

- Symantec AntiVirus Corporate Edition version 10.x
- Symantec Endpoint Protection Client 11.x
- Symantec Endpoint Protection Small Business Edition (V12)
- McAfee VirusScan Enterprise version 8.5.0i
- McAfee VirusScan Enterprise version 8.7i
- Microsoft Forefront Client Security version 1.x
- Sophos Endpoint Security and Control 9
- Trend Micro OfficeScan 10.5

⚠ Note: *These products must be provided by the customer. Load only the client software.*

1.5. Definitions

- **LiveUpdate** – A feature that allows servers and clients to retrieve updates from an internal server or Symantec's official LiveUpdate 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.
- **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. These clients must download their own virus definition updates.

2. Customer Preparation Checklist

Prior to beginning the installation, note the following:

- Hologic does not supply antivirus software. It is the customer's responsibility to procure the software and associated licenses.
- Customers who want to use the Symantec AntiVirus Corporate Edition must provide their own Symantec AntiVirus Server within their networked environment. Only client software should be loaded on SecurView systems. The clients will retrieve updates from their existing Symantec AntiVirus 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.

3. Preinstallation Checklist

Prior to beginning the installation, review the following:

- Ensure no existing antivirus software is loaded on the workstation prior to installation.
- Ensure the installer has the proper serial keys and associated licenses for the product that is to be installed.

4. Installing Symantec AntiVirus Corporate Edition v10.x as Unmanaged Client

- 1 On the workstation, log into Windows as a user that has administrator privileges (e.g., **Customer**).
- 2 Install the software:
 - a Insert the Symantec AntiVirus Corporate Edition v10.x media.
 - b Browse to the media 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 'Welcome to the InstallShield Wizard for Symantec AntiVirus' appears, click **Next**.
 - f Click 'I accept the terms in the license agreement'. A window appears, prompting you to choose one of two options. **Client install** and **Server install**.
 - g Select **Client install** and proceed to the next window.
 - h Click the **Complete** check box, then click **Next**.
 - i Select **Unmanaged** and click **Next**.
 - j Ensure **Auto-Protect** and **Run-LiveUpdate** are checked and proceed to the next section by clicking **Next**.
 - k Click **Install**.
 - l After the installation completes, click **Finish**.
- 3 Configure Symantec AntiVirus Corporate Edition v10.x:
 - a Double-click the Symantec shield in the system tray to open the Symantec AntiVirus console.

- b You should be presented with a window that displays '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 to the C: drive or drive where Symantec is installed.
 - f Select **Browse** and locate the .sfl you placed on the C: drive.
 - g Click **Next**.
 - h Close the Symantec AntiVirus console.
- 4** Configure Real-time Protection (Auto-Protect):
- a Double-click the Symantec shield in the system tray to open the Symantec AntiVirus console.
 - b From the top of the window, select **Configure > File System Auto-Protect**.
 - c Under 'File types' change the setting from 'All types' to 'Selected'.
 - d For optimal performance, exclude the following directories and their subdirectories from scanning:
 - C:\Postgresplus
 - C:\Program Files\Microsoft SQL Server
 - E:\MSSQLSERVER
 - E:\Securview
 - F:\DICOM
 - F:\DICOM_spool
 - F:\Images
 - F:\PrintSpool
 - F:\TomolImages

Note: If the above drive letters do not apply to your configuration, please substitute the appropriate drive letters.

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 workstation, leave 'All types' checked. This may degrade performance on your workstation.

5. Installing Symantec Endpoint Protection Client 11.x as Unmanaged Client

- 1 On the workstation, log into Windows as a user that has administrator privileges (e.g., **Customer**).
- 2 Install the software:
 - a Insert the Symantec media.
 - b Browse to the media and double-click **setup** to start the installation process.
 - c When the window appears, click **Install Symantec Endpoint Protection Client**.
 - d A window appears. Click **Next**.
 - e Click 'I accept the terms in the license agreement', then click **Next**.

- f Select **Unmanaged client** and proceed to the next window.
 - g Select **Custom** and click **Next**.
 - h Do not install the following components: **Network Threat Protection** and **Application and Device Control**.
 - i Click the drop-down menu in front of **Network Threat Protection** and select **x**.
 - j Click the drop-down menu in front of **Application Threat Protection** and **Device Control** and select **x**.
 - k Click **Next**.
 - l Ensure the **Enable Auto-Protect** and **Run LiveUpdate** boxes are checked, then click **Next** twice.
 - m Click **Finish**.
 - n You are now looking at the Symantec Endpoint Protection dashboard. Ensure there is no warning about out-of-date definitions. If there is a warning, please work with your local IT group to configure the system before clicking **Fix**, which requires an active Internet connection to download the definition files from Symantec.
- 3 Configure protection (balancing security with performance).
- a Click the **Change settings** tab located on the left side pane of the Symantec Endpoint Protection dashboard.
 - b Click **Configure Settings** next to the 'Antivirus and Antispyware Protection' field.
 - c Click the **File System Auto-Protect** tab, then click the **Selected** radio box under the 'File Types' section. Click **OK** to close out.
 - d Click the **Change settings** tab located on the left side pane of the Symantec Endpoint Protection dashboard.
 - e Click **Configure Settings** next to the 'Centralized Exceptions' field.
 - f Click **Add →Security Risk Exceptions→Folder**.
 - g For optimal performance, exclude the following directories and their subdirectories from scanning:
 - C:\Postgresplus
 - C:\Program Files\Microsoft SQL Server
 - E:\MSSQLSERVER
 - E:\Securview
 - F:\DICOM
 - F:\DICOM_spool
 - F:\Images
 - F:\PrintSpool
 - F:\Tomolimages

Note: *If the above drive letters do not apply to your configuration, please substitute the appropriate drive letters.*

6. Installing Symantec Endpoint Protection Small Business Edition (v12)

Note: Symantec Endpoint Protection Small Business Edition is best used in a client-server setup where the Symantec internal server provides protection to the systems on the local network. Hologic assumes the customer is already running a Symantec server and adding the Hologic system as one of its protected nodes.

For optimal performance, please make sure Symantec excludes the following directories and subdirectories from scanning on the client system:

- C:\Postgresplus
- C:\Program Files\Microsoft SQL Server
- E:\MSSQLSERVER
- E:\Securview
- F:\DICOM
- F:\DICOM_spool
- F:\Images
- F:\PrintSpool
- F:\TomolImages


Note: If the above drive letters do not apply to your configuration, please substitute the appropriate drive letters.

Only 'Virus and Spyware policy- High performance' should be activated on Hologic systems for optimal patient care. Furthermore Hologic recommends turning the firewall and intrusion policies off unless the customer has a knowledgeable local IT staff to provide support and maintenance.

7. Installing McAfee VirusScan Enterprise v8.5.0i

- 1 On the workstation, log into Windows as a user that has administrator privileges (e.g., **Customer**).
- 2 Install the software:
 - a Insert the McAfee v8.5.0i media.
 - b Browse to the media and launch the setup icon from there.
 - c Click **VirusScan v8.5.0i for Win NT/2k/XP**.
 - d Click **Install VirusScan v8.5.0i**.
 - e Click **Next**.
 - f Select the appropriate licensing information, click **I accept**, then click **OK**.
 - g Select **Typical** installation and click **Next**.
 - h Click **Install**.
 - i When installation is complete, deselect **Update Now** and **Run On-Demand Scan**.
 - j Click **Finish**.
 - k Reboot the system, if you are prompted.

- 3 Configure McAfee v8.5.0i:
 - a After the workstation boots back into Windows, log in as the same user that has administrator privileges (e.g., **Customer**).
 - b Double-click the McAfee shield in the system tray and select **Properties**.
 - c In the left window, click **All Processes**.
 - d Click the **Detection** tab at the top. Select **On Network Drives**.
 - e Click the **Advanced** tab at the top.
 - f Under compressed files, select **Scan inside archives** then select **Decode MIME encoded files**.
 - g Click **Apply** and exit the console.
- 4 Exclude folders:
 - a Double-click the McAfee shield in the system tray and select **Properties**.
 - b For optimal performance, exclude the following directories and their subdirectories:
 - C:\Postgresplus
 - C:\Program Files\Microsoft SQL Server
 - E:\MSSQLSERVER
 - E:\Securview
 - F:\DICOM
 - F:\DICOM_spool
 - F:\Images
 - F:\PrintSpool
 - F:\TomolImages

 **Note:** If the above drive letters do not apply to your configuration, please substitute the appropriate drive letters.

8. Installing McAfee VirusScan Enterprise v8.7.x

- 1 On the workstation, log into Windows as a user that has administrator privileges (e.g., **Customer**).
- 2 Install the software:
 - a Insert the McAfee v8.7.x media.
 - b Browse to the media and double-click **setupvse.exe** to start the installation process. The McAfee console should appear.
 - c Click **Next** at the McAfee VirusScan Enterprise Setup screen.
 - d Select the appropriate licensing information, click **I accept**, then click **OK**.
 - e Select **Typical** and click **Next**.
 - f Choose 'Protection Level Standard' and click **Next**.
 - g Click **Install**.
 - h When installation is complete, deselect **Update Now** and **Run On-Demand Scan**.

- i Click **Finish**.
- j Reboot the system, if you are prompted.
- 3 Log back into Windows as the same user with administrator privileges (e.g., **Customer**) and proceed with configuration:
 - a Double-click the McAfee shield in the system tray and select **Properties**.
 - b In the left pane, click **All Processes**, then the **Exclusions** tab.
 - a Add the following directories and their subdirectories to Exclusions:

C:\Postgresplus
C:\Program Files\Microsoft SQL Server
E:\MSSQLSERVER
E:\Securview
F:\DICOM
F:\DICOM_spool
F:\Images
F:\PrintSpool
F:\TomolImages

Note: Don't forget to check the **Also exclude subfolders** box when you add directories to Exclusions.

Note: If the above drive letters do not apply to your configuration, please substitute the appropriate drive letters.

9. Installing Microsoft Forefront Client Security v1.x

Note: Microsoft Forefront Client security is an IT-centric product that is geared toward Enterprise with IT staff. Hologic assumes the customer is already running one or more server-topology in their IT infrastructure environment.

For optimal performance, be sure the installed antivirus software excludes the following directories and their subdirectories from scanning:

C:\Postgresplus
C:\Program Files\Microsoft SQL Server
E:\MSSQLSERVER
E:\Securview
F:\DICOM
F:\DICOM_spool
F:\Images
F:\PrintSpool
F:\TomolImages

Note: If the above drive letters do not apply to your configuration, please substitute the appropriate drive letters.

10. Installing Sophos or Trend Micro Antivirus

Note: *Sophos and Trend Micro are IT-centric products that are geared toward Enterprise with IT staff. Hologic assumes the customer has the infrastructure already running and the personnel with expertise to deploy and manage the antivirus product and only need to know which files or directories on Hologic systems to exclude from scanning.*

Only antivirus features install is recommended. Other features such as firewall or application control, etc. are not recommended as they may increase the risk to loss of productivity due to the high maintenance required to care for them properly. Install them at your own risk if you have the local personnel with the right skill set to configure and maintain them.

For optimal system performance, please ensure the installed antivirus software excludes the following directories and their subdirectories from scanning:

- C:\Postgresplus
- C:\Program Files\Microsoft SQL Server
- E:\MSSQLSERVER
- E:\Securview
- F:\DICOM
- F:\DICOM_spool
- F:\Images
- F:\PrintSpool
- F:\TomolImages

Note: *If the above drive letters do not apply to your configuration, please substitute the appropriate drive letters.*

11. Manually Installing Symantec AntiVirus Corporate Edition v10.x Updates

- 1 Download virus definitions when SecurView 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 media of your choice (e.g., thumb drive, network share drive, download and then burn to a CD).
- 2 Manually install the updates:
 - a On the workstation, log into Windows as a user that has administrator privileges (e.g., **Customer**).
 - b Load the file containing the virus definitions and double-click the executable. A window will appear and ask 'Do you want to update your virus definition files?'
 - c Click **Yes**.
 - d After installation is complete, you will be presented with a window. Read the contents of the message and click **OK**.
 - e Reboot the workstation, if you are prompted.

Note: *'Unmanaged clients' must obtain their virus definition updates from Symantec. The above process may differ slightly for each Symantec product.*

12. Manually Installing McAfee Updates

- 1 Download virus definitions when SecurView does not have Internet access:
 - a Use a PC with Internet access and browse to:
<http://www.mcafee.com/us/small/downloads/index.html>
 - b Locate and download the appropriate DAT files to the media of your choice (e.g. thumb drive, network share drive, download and then burn to a CD).
- 2 Manually install the updates:
 - a On the workstation, log into Windows as a user that has administrator privileges (e.g., **Customer**).
 - b Load the file containing the virus definitions and double-click the executable.
 - c A window will appear. Click **Next**.
 - d After the installation completes, click **Finish**.

13. System Testing

Use this section to ensure proper installation of the antivirus software utility. Incorrect installation may compromise system stability. In addition, for antivirus software utilities to remain effective, they must be updated regularly. The system regression tests outlined in this section should be completed by the customer after the antivirus software utility is installed or updated. If the following performance tests are inconclusive or fail, please contact Hologic Customer Service before placing the system in use.

13.1. Receiving Images

- 1 From an external source (e.g., Selenia Acquisition Workstation), send five studies to SecurView.
- 2 Ensure that the studies are received in a time period consistent with the baseline configuration number recorded in the Patch Installation section of the corresponding SecurView Cybersecurity Product Report.

13.2. Loading Images

- 1 From an external source, send five studies to SecurView.
- 2 While the studies are being received, open a patient for review.
- 3 Ensure that the image loading time is consistent with the baseline configuration number recorded in the Patch Installation section of the corresponding SecurView Cybersecurity Product Report.

13.3. CPU Monitoring

- 1 Log into Windows as the user that runs the SecurView application (e.g., **scr**).
- 2 Log into the application as **admin**.
- 3 Click **Exit to Windows**.
- 4 Press the **Windows** key and right-click the taskbar.
- 5 Select **Task Manager**.
- 6 Once the Task Manager is present, click **Options >** and select **Always on Top**.

- 7 Restart the application and log in as **review**.
- 8 With the Task Manager window open, open a patient to review images.
- 9 Ensure **CPU usage** is below 30%.

⚠ Note: *CPU spikes are normal, but sustained high CPU usage for no apparent reason is not. To optimize performance, schedule the system scan during non-peak or after hours.*

Hologic Inc.
35 Crosby Drive
Bedford, MA 01730-1401 USA
Tel: +1.781.999.7300
Sales: +1.781.999.7453
Fax: +1.781.280.0668

Hologic N.V.
Authorized Representative
Leuvensesteenweg 250A
1800 Vilvoorde, Belgium
Tel: +32.2.711.4680
Fax: +32.2.725.2087

For more information about Hologic products, services, and facilities, visit www.hologic.com.