Symantec 10.0, McAfee 8.0i and McAfee 8.5i anti-virus installation

Purpose:

To install anti-virus software on the existing SecurView Workstation 5-X products.

Scope:

This document applies to all SecurView products with version 5-X software.

Estimated Time:

Installation of anti-virus products will take the network 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
Option 1: Symantec Anti-virus Corporate Edition 10.0	**Customer provided. Only the client of the Corporate edition is loaded on our products**
Option 2: McAfee 8.0i	**Customer provided. Only the client of the Corporate edition is loaded on our products**
Option 3: McAfee 8.5i	**Customer provided. Only the client of the Corporate edition is loaded on our products**

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 scans the header of each file to determine its extension and to identify possible malicious code.

Smartscan – A scanning technique that scans the header of each file to determine it's true file extension and to identify possible malicious code.

Stand Alone Workstation – A single workstation.

Unmanaged – The clients do not connect to the network nor do they have a parent server with which they communicate with. These clients must download their own virus definition updates.

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 software of choice. Hologic does not supply the customer with this software, it is the customer's responsibility to purchase the software and associated licenses.
- For customers wanting to use the Norton Corporate Edition, they must provide their own Symantec Norton Server within their networked environment. Only client software should be loaded on the Securview. 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.

2.0 Pre-installation Checklist

Prior to beginning the installation, review the following:

- Ensure no existing anti-virus 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.

3.0 Installing Symantec Anti-virus 10.0 as an unmanaged client

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

1. **On the workstation, login to Windows as Administrator.**
2. **Installation procedures:**
   a. Insert the "Symantec Anti-virus 10.0" cd from the Symantec Anti-virus 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 Anti-virus."**
   d. A second window will appear. Again, select **"Install Symantec Anti-virus."**
   e. When the **"Welcome to the InstallShield Wizard for Symantec Anti-virus"** 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 is checked and proceed to the next section by clicking **"Next."**
   l. Click the **"Install"** button.
   m. After the installation completes, click **"Finish."**

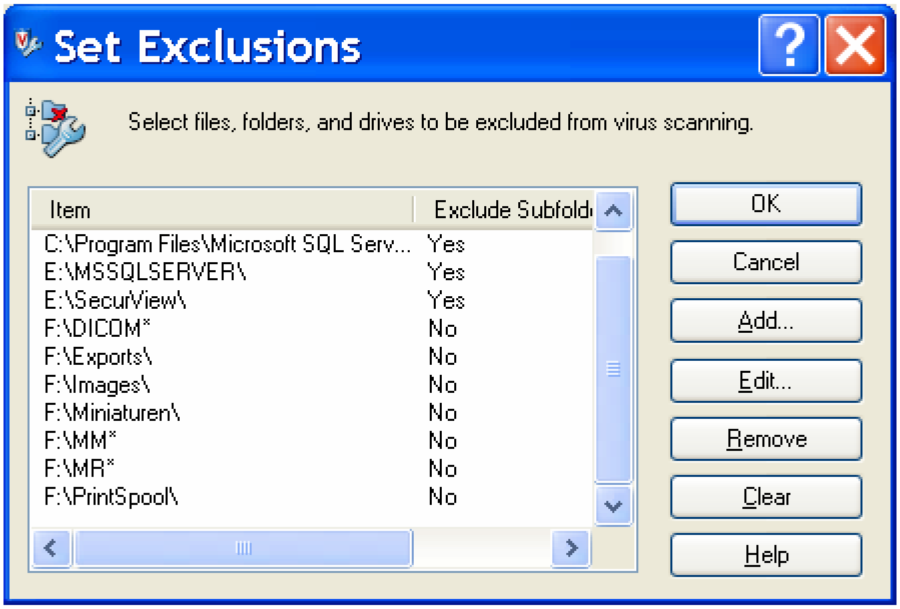
3. **Configuring Symantec Anti-virus 10.0**
   a. Double click the shield on your system tray to bring up the Symantec Screen
   b. You should be presented with a window that states, **"License not found."**
   c. Click the hyperlink http://licensing.symantec.com/
   d. Enter your serial number and click **NEXT**. You should receive a .sfl file via email. If you do not, contact Symantec Technical Support.
   e. Copy the **.sfl file** over to the C: drive
   f. Select "BROWSE" and locate the .sfl you placed on your C: drive.
   g. Click **"Next."**
   l. Close the Symantec Anti-virus 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."**

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 files" checked. This may degrade performance on your workstation.*

4.0 Installing McAfee 8.0i

1. **On the workstation, 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 workstation 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."
    g. Click "Apply" and exit the console.

4. **Excluding Folders**
    a. Double click the McAfee shield in the system tray and choose "Properties."
    b. Exclude the following files:


Set Exclusions

Select files, folders, and drives to be excluded from virus scanning.

Item	Exclude Subfold
C:\Program Files\Microsoft SQL Serv...	Yes
E:\MSSQLSERVER\	Yes
E:\SecurView\	Yes
F:\DICOM*	No
F:\Exports\	No
F:\Images\	No
F:\Miniaturen\	No
F:\MM*	No
F:\MR*	No
F:\PrintSpool\	No

5.0 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 Overlow 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 teh 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)

6.0 Manually installing updates

Symantec and Norton

1. **Downloading virus definitions when the 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 desktop
   c. When the download completes, burn the executable to a CD.
2. **Manually installing the updates**
   a. On the workstation, 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 workstation 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."*

7.0 Manually installing updates

McAfee

3. **Downloading virus definitions when the SecurView 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 workstation, 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."
   e. When it is finished, click "FINISH."

8.0 System Testing

The objective of this section is to ensure the proper installation of the anti-virus software utility. Incorrect installation may compromise system stability. Additionally for anti-virus software utilities to remain effective, they must be regularly updated. The system regression tests outlined in this section should be successfully completed by the user after the anti-virus 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.
.

1. **Receiving images**
   a. From an external source (e.g. Selenia Acquisition Station) send 5 studies to the SecurView.
   b. Ensure that the studies are received in a time period consistent with the baseline configuration number

2. **Loading images**
   a. From an external source (e.g. Selenia Acquisition Station) send 5 studies to the SecurView.
   b. While the studies are being received, load a study.
   c. Ensure that loading time is **consistent with** the recorded baseline configuration number.

3. **CPU Monitoring**
   a. Log in to the application as “**admin**.”
   b. Click “**EXIT TO WINDOWS**”
   c. Press the **Windows key** and right click the taskbar
   d. Choose “**Task Manager**.”
   e. Once “Task Manager” is present, click Options > and choose “**Always on Top**.”
   f. Restart the application and log in as **review**
   g. With the “Task Manager” window open, load images
   h. Ensure **CPU usage** is below 30%

Note *CPU spikes are normal, sustained usage past 50% is not.*

4. **Slow Performance**

   a. If you experience degraded performance, ensure that Autoprotect is configured with “**Selective Scanning**.” (See sections 2 and 3)