



Product Bulletin

Bulletin Number: P-2009-0039-Global-Rev4
Date: 17 February 2011

CallPilot Support for Anti-Virus Applications

REVISION HISTORY

Date	Revision #	Summary of Changes
03 April 2009	Original bulletin	This is the original publication.
17 August 2009	Rev. 1	Updated to include refined installation and configuration guidelines for McAfee 8.0i.
25 August 2009	Rev. 2	Updated to improve consistency for McAfee 8.0i CPU utilization threshold setting.
15 December 2009	Rev. 3	Updated to add McAfee 8.7 support and clarify some settings within eTrust Anti-Virus 8.1.
17 February 2011	Rev. 4	Updated to introduce compatibility with TrendMicro OfficeScan 10.5

Introduction

This bulletin provides installation and configuration support of the latest anti-virus applications for use with CallPilot, specifically Computer Associates™ eTrust Antivirus 8.1, McAfee™ VirusScan Enterprise 8.7, Symantec™ End-Point Protection 11, and Trend Micro™ OfficeScan 10.5

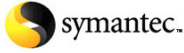
CallPilot, when properly installed and maintained, is not generally susceptible to viruses. Avaya understands the importance of safeguarding such a mission-critical application from the possibility of an attack. CallPilot has been tested with and supports some industry-leading anti-virus (AV) applications for installation and use on the CallPilot server. Use of an anti-virus application as well as following the “Best Practices” suggestions listed below, help to ensure CallPilot servers remain virus-free.

Note: Each anti-virus application has specific configuration and operation requirements as documented in the appendices. These configuration guidelines must be followed to avoid CallPilot service degradation or outages.

Supported Anti-Virus Applications

The following table identifies industry leading anti-virus applications used today within most customer IT environments. Avaya does not make any recommendations for any of the applications listed; only that each has been tested and verified to function properly with the CallPilot release as noted.

If older versions of either the anti-virus applications or CallPilot software releases are needed, reference bulletins P-2007-0101-Global (rev-1 latest) or P-2003-0151-Global (rev-4 latest) for installation and configuration details.

Vendor	Application Name	Version	Notes	Supported CallPilot Release
 Computer Associates™	eTrust Antivirus	8.1		4.0, 5.0
 A Network Associates Business	VirusScan Enterprise	8.7	1	4.0, 5.0
 symantec.	End-Point Protection	11		4.0, 5.0
 TREND MICRO™	OfficeScan	10.5		5.0

Notes:

1. When using McAfee AntiVirus, it's recommended to set the CPU utilization to **70%**. This balances CallPilot operation with an acceptable duration of time for completing virus scans on the server. Please see [Appendix-C](#) for detailed instructions.
2. CallPilot 4.0 JITC Hardened Configuration servers support the same anti-virus applications as non-JITC servers.
3. As newer sub-release versions of the above applications are made available, support for those versions is implied. For example, Symantec End-Point 11 includes sub-releases 11.0.1, 11.0.2, etc.
4. As newer release versions are made available, support will be added once testing and trials are completed, generally within six (6) months of release. This bulletin will be re-issued announcing changes as necessary.

Best Practices

In addition to those practices outlined in the NTPs (the most current revisions for each release are available on the Avaya Support Portal at <https://support.avaya.com/css/Products/P0712>, the following practices should also be adhered to:

- All PEP files, CD-ROMs, DVD-ROMs, USB-attached disk drives (CallPilot 5.0 only), and floppy disks should be scanned prior to installation or upload to the server in order to ensure they are virus free.
- Do not “surf the web”, run downloaded programs, access personal e-mail accounts, or other potentially hazardous activities from the CallPilot server.
- CallPilot utilizes Windows accounts for operation. While some accounts must not be changed or they will impact operation, the following well-known account passwords should be changed from their defaults to secure, strong passwords: Administrator, NGenSys, NGenDist, NgenDesign, and gamroot (if equipped with RAID using the AcceleRAID-352 RAID controller).
- Avoid mapping remote drives onto a CallPilot server or mapping a CallPilot server’s drives onto another server. If drives are mapped for maintenance/backup purposes, disconnect them as soon as possible when no longer needed.
- Remote-disk (LAN) backups utilize mapped drives. All mapped drives should be disconnected when not actively being used for either backing up or restoring a system.
- Ensure Microsoft Operating System (OS) updates are up-to-date according to instructions in the “CallPilot Server Security Update” bulletin. Reference Product Bulletin *CallPilot Server Security Update-2011* (revised periodically) for a list approved Microsoft security updates and CallPilot hardening PEPs.

Implementing Anti-Virus Applications on CallPilot

Anti-virus applications can impact the performance of server-based applications like CallPilot. It is essential to follow the configuration guidelines that appear in the Appendices to this bulletin. The anti-virus application is not available from nor supplied by Avaya; it is customer-supplied. It is also important to consider the general guidelines listed below:

- Anti-virus applications should only be installed in the following disk locations to ensure sufficient disk space remains available for required system operations such as upgrades and general maintenance activities:
 - o 4.0 and earlier should use the D: drive
 - o 5.0 and later should use the C: drive
- Ad-hoc or scheduled scanning of the CallPilot server should only be done during low traffic times and not between midnight to 04:00 a.m. (which would conflict with the regular CallPilot audits).
- The anti-virus application should be configured to automatically retrieve virus definition updates at least weekly during off-hours. Current definitions are critical in properly protecting the server.
- The anti-virus application should be configured to check for viruses whenever certain types of files are modified (incoming files). Relying only on periodic scans of the server hard drives could allow a virus considerable time to do damage (i.e. the time from when the virus first infects the system until the scan is done). This feature is referenced differently by each application as follows:
 - o "Real Time Monitor" by Computer Associates eTrust InoculateIT
 - o "On-Access Monitor" by McAfee Netshield
 - o "File System Real-time Protection" by Symantec Norton Anti-Virus

- If viruses are discovered on the server and the anti-virus software suggested solution is to replace the infected files, **DO NOT** attempt to manually remove or replace affected files. Allow the anti-virus application to perform its actions to correct the infection. If problems arise afterwards, contact Avaya Technical Support for additional support.
 - o Depending on the virus infection and corruption introduced, it may be required to perform a full system backup, re-install the system from scratch, and then recover the database, mailboxes, and messages from the backup.
- During virus eradication, it is recommended the server be isolated from the network by disconnecting both the ELAN and CLAN to prevent further propagation of the virus.

Alternatives to Installing Anti-Virus Applications

If use of the applications mentioned above is not desired, virus scanning of the server can still be accomplished, albeit with far less protection, using the following steps:

1. Install the Anti-Virus software on a separate Windows Workstation on the Customer Local Area Network (CLAN).
2. On the CallPilot server, share each of the drives with read-only permissions
3. During an off-peak period of the day, login to the Windows Workstation where the anti-virus software is installed and map to the CallPilot server drives using Microsoft Networking. When asked for a user ID and password, use NGenSys or NGenDist.
4. Scan the mapped CallPilot server drives from the Windows Workstation.

Note: Anti-virus software should not be configured to automatically delete infected files.
5. Once the scan completes, un-map the drives and remove sharing from the CallPilot server drives.

Note: Sharing connections should always be removed immediately when scanning is not actively taking place.
6. Ad-hoc scanning at regular intervals during off-hours is preferred.

What does this mean to customers?

To ensure CallPilot servers are protected now and into the future, customers are provided both on-server and off-server anti-virus alternatives. Avaya is hopeful that these provide an enhanced “fit” within customer IT environments.

Testing Anti-Virus applications

To ensure anti-virus applications are installed and functioning correctly, it is recommended to use a test virus available for download from <http://www.eicar.org>. This is not an actual virus, but contains specific codes recognized by anti-virus applications for the specific purpose of testing.

If the anti-virus application has been installed and configured correctly, on-access (real-time) monitoring should detect the virus before it is stored on the CallPilot server hard drive. If remote scanning is being utilized, the test virus file should be detected during any scanning activity.

Also, to ensure the anti-virus application is functioning, it's recommended to review the scan statistics provided by each application. If properly configured, the statistics for number of files scanned by the on-access/real-time monitoring may or may not show files being scanning during normal CallPilot usage scenarios depending on configured features. To test that on-access/real-time scanning is working, check the statistics (# of files scanned), copy a file onto the server (or create a new one), then review the statistics again. The count for files scanned should have increased as a result of the file AV scan.

Documentation

For more information regarding Installation and Configuration of supported anti-virus applications, refer to the following appendix sections of this bulletin depending on which application is being used:

[Appendix-A: Computer Associates' eTrust AntiVirus 8.1](#)

[Appendix-B: McAfee VirusScan Enterprise 8.5](#)

[Appendix-C: McAfee VirusScan Enterprise 8.7](#)

[Appendix-D: Symantec EndPoint Protection 11](#)

[Appendix-E: Trend Micro OfficeScan 10.5](#)

Note: If your desired anti-virus application version is not listed above, reference the installation and configuration information guidelines as documented in one the following product bulletins:

- P-2007-0101-Global-Rev1 *CallPilot Support for Anti-Virus Applications*
 - o Computer Associated eTrust Anti-Virus 7
 - o Symantec AntiVirus 10
 - o Trend Micro OfficeScan 7.0
- P-2003-0151-Global-rev 4 (and earlier) *CallPilot Support for Anti-Virus Applications*
 - o Computer Associates eTrust InoculateIT 6 and 4.53
 - o McAfee Netshield for WinNT 4.5
 - o McAfee VirusScan Enterprise 7.x
 - o Symantec AntiVirus 9.0, 8.1 (Corporate Edition)
 - o Symantec Norton AntiVirus 7.x (Corporate Edition) and 2001
 - o Trend Micro ServerProtect 5.58
- 2002-035 *CallPilot 1.07 Support for Anti-Virus Applications*
- 2000-087 *Guidelines for use of Anti-virus software with CallPilot servers*
- 99067 *CallPilot Unauthorized Hardware and Software*

eTrust InoculateIT and eTrust AntiVirus are registered trademarks for Computer Associates
Norton AntiVirus and Symantec AntiVirus are registered trademarks for Symantec Corporation
NetShield and VirusScan Enterprise are registered trademarks for McAfee
ServerProtect and OfficeScan a registered trademarks for Trend Micro

Appendix-A

This appendix provides Installation and Configuration procedures for CallPilot 4.0 and 5.0 servers utilizing the **Computer Associates Antivirus 8.1** anti-virus application.

Product Features:

- Able to scan inside compressed files.
(May not be able to handle all compression types, however.)
- Able to block all files based on file-type.
(This may provide a way to handle password-protected zip files.)
- Able to scan NTFS alternate data streams.
- Performs memory, boot sector and disk scanning.
- Antivirus scans and virus definition updates work properly even when the local console is in a logged-out state.

Product Deficiencies:

- System reboot may be required after install. Maintenance window is needed.
- Real-time monitoring cannot scan incoming files only.
- Real-time scanning exclusions only on a file type or directory basis. Cannot exclude specific files or use wild-card characters.
- Browser-based GUI is slow on some CallPilot servers and is somewhat confusing.
- Does not generate any events in Windows event log, but rather has a separate logging subsystem.

Product Tested:

- Computer Associates Antivirus 8.1 Integrated Threat Management (ITM) trial version (also called eTrust Antivirus).

Note: CA PestPatrol (anti-spyware product), CA Secure Content Manager, and CA Host Based Intrusion Protection System were not tested and are not authorized for installation on CallPilot servers.

Installation and Configuration Guidelines:

Use a fully patched and anti-virus protected PC to download the latest AV software and virus definitions and burn the files onto a CD-ROM so that it can be brought to the CallPilot server without using the network. It is dangerous to use the Internet to download the initial virus definitions after a fresh install of Anti-Virus software. An unprotected computer can become infected in the time it takes to download updates.

For eTrust Antivirus, definitions and updates can be downloaded from:

<http://www.ca.com/securityadvisor/virusinfo/signaturefiles> (URL is subject to change)

Select "CA Anti-Virus 7.1 and newer Beta Signatures", agree to the "disclaimer" and you get to an ftp site. Select "ITM" (<ftp://ftp.ca.com/pub/inoculan/scanengbeta/ITM>), and then scroll to the bottom of the list to find the most recent signature file. Download a file with a name such as "vet_full_5872.pkg". This file is actually a compressed archive. It can be opened with a program such as WinZip. Extract the contents of the archive: two files with names such as "causign.xml" and "fv_x86_5872.exe". (The four digit number in the fv filename changes

according to the signature version.) Burn these two files onto a CD (or, if the CallPilot supports USB, you can use a USB drive. Since files are over 10 MB in size they will not fit on a floppy.)

For best security, a CallPilot server must never be connected to the Internet unless it has the latest CallPilot OS Security PEPs, all OS hotfixes authorized for CallPilot and has Anti-Virus software installed with the latest virus definitions. Therefore, unless the network is very well-protected, disconnect the CallPilot Server from the network by unplugging both ELAN and CLAN cables before installing the Anti-Virus Software. Be sure you remember where the cables should be plugged back in.

Uninstall any existing Anti-Virus software. Problems will occur if more than one anti-virus product is installed at a time. Reboot if required.

Before installing Antivirus software - install all applicable CallPilot OS Security PEPs from CD. Install any additional, authorized hotfixes from CD. Your installation of the Antivirus software should also be done from CD so that the network can be connected only when the system is fully protected.

If installed according to the instructions given here, antivirus software should have no noticeable impact on CallPilot performance and capacity for normal messaging-related operations. Certain exceptional operations that involve reading or updating a large number of files may operate significantly slower on some platform types due to the added cost of virus scanning. Examples are: software upgrades, PEP installs, backup, restore from backup. You may want to temporarily disable Realtime monitoring while performing those operations.

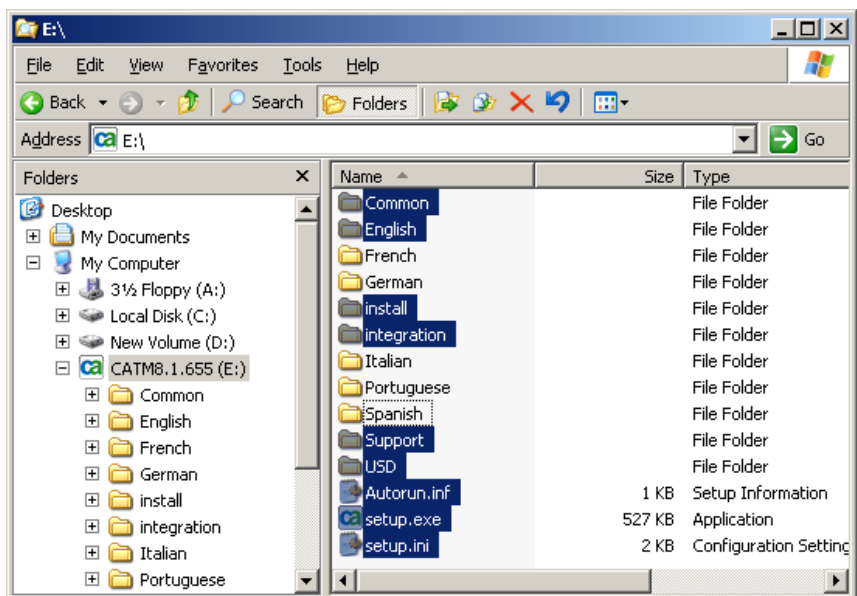
Note: The CA Antivirus GUI works best when display resolution is set to 1024x768 or higher.

Installation of CA Integrated Threat Management (ITM) Product

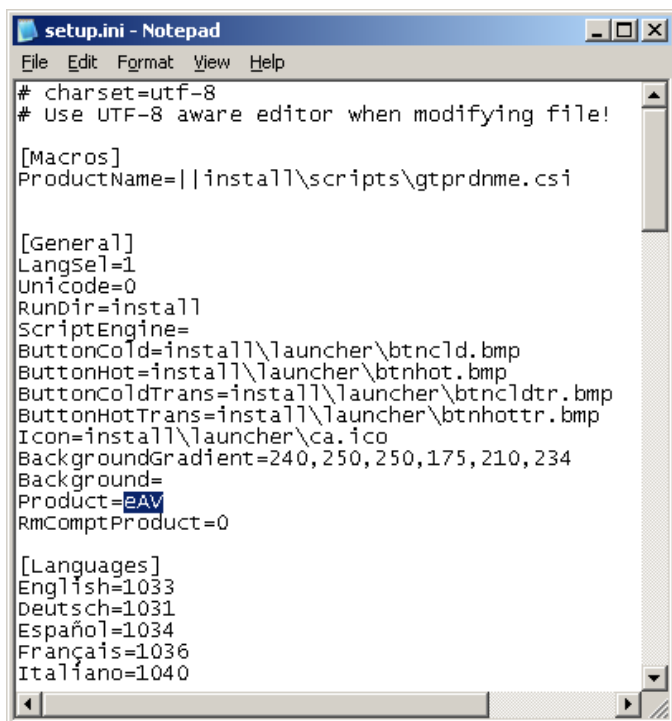
CA sells a product named "CA eTrust Integrated Threat Management Suite r8.1". This product includes both CA Antivirus and CA's anti-spyware product called "PestPatrol". Avaya has not qualified PestPatrol on CallPilot servers; therefore it must not be installed.

If you are installing using the CA ITM product, you need to edit the setup.ini file so that only the Anti-Virus product will be installed. (If the product you are installing only includes AV, then this step is not necessary.)

Since the installation CD is read-only, setup.ini will need to be edited while it resides on a hard disk. You can edit it on a separate desktop PC then burn the entire modified product onto a CD to bring to the CallPilot server. Alternatively, assuming adequate disk space on the CallPilot server (652 MB needed), you can copy the installation CD to a temp folder on the CallPilot server, edit the setup.ini file there, then run the install from the temp folder. Be sure to delete the installation files from the temp folder when done since they consume a lot of space (and will also slow down any AV scan done on the server). (NOTE: when copying the CA ITM installation, you can omit unneeded language files such as the French, German, Italian, Portuguese and Spanish folders to reduce the disk space needed to 530 MB.)



Edit setup.ini using Notepad. Look for a line “Product=ITM”. Edit this to read “Product=eAV” and then save and quit out of notepad.

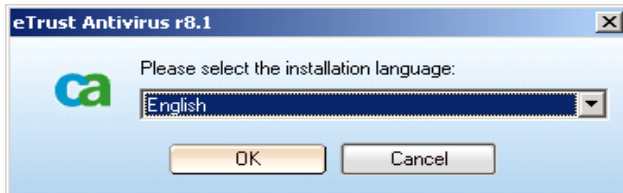


Licensing CA AntiVirus

In order for the AntiVirus software to continue working, it must be a properly licensed version. You can install without a license but then you will have only a 30 day trial. If you install the software in trial mode, you can later import a license file to turn the trial software into a fully licensed version.

Step by Step Installation Instructions

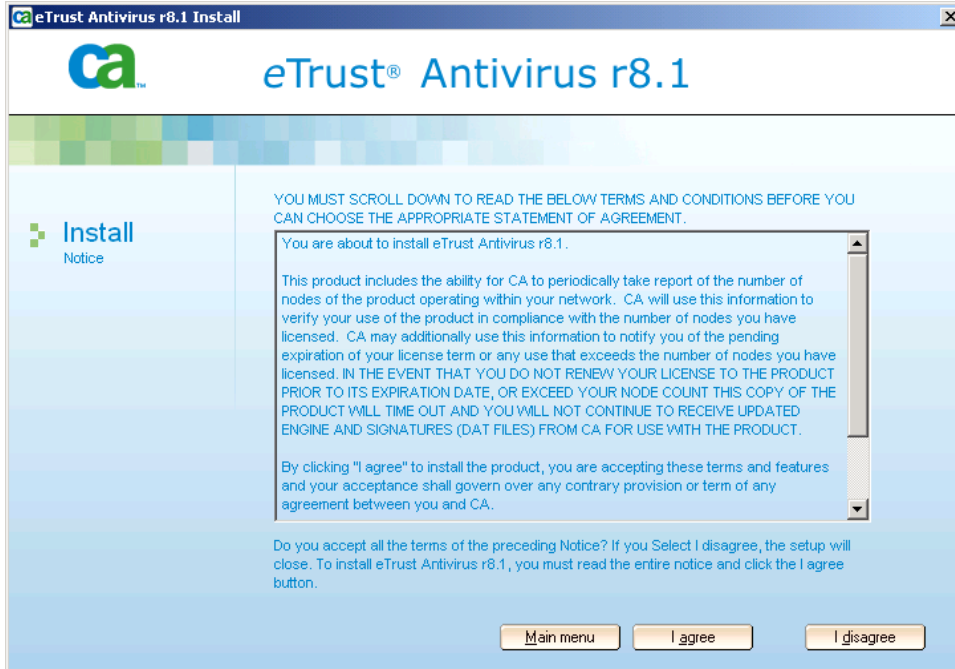
1. Insert the CA Anti-virus 8.1 CD and begin installation by double-clicking “**SETUP.EXE**”.



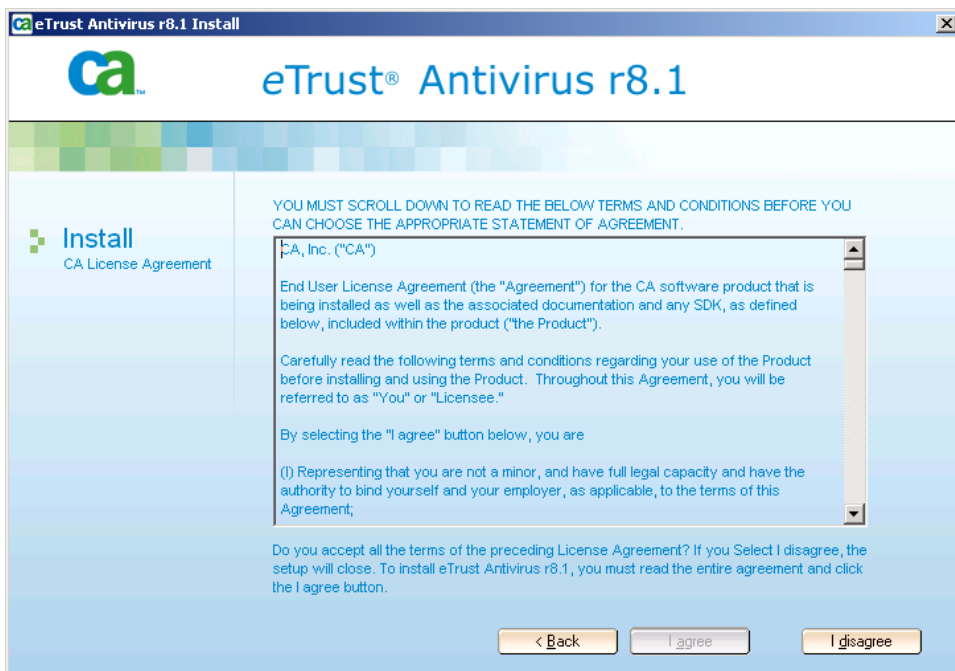
2. Select English and click “**OK**”.



3. Click “**Install**”.



4. Scroll down to read the text and then click **"I agree"**. A second EULA is displayed

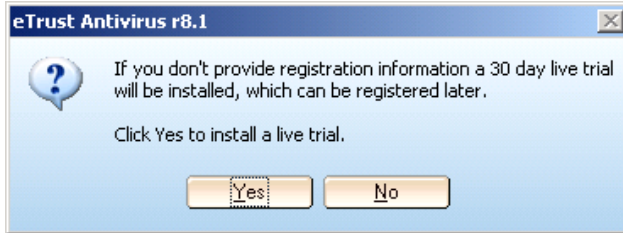


5. Scroll down to read it all, and then click **"I agree"**. A third EULA is displayed

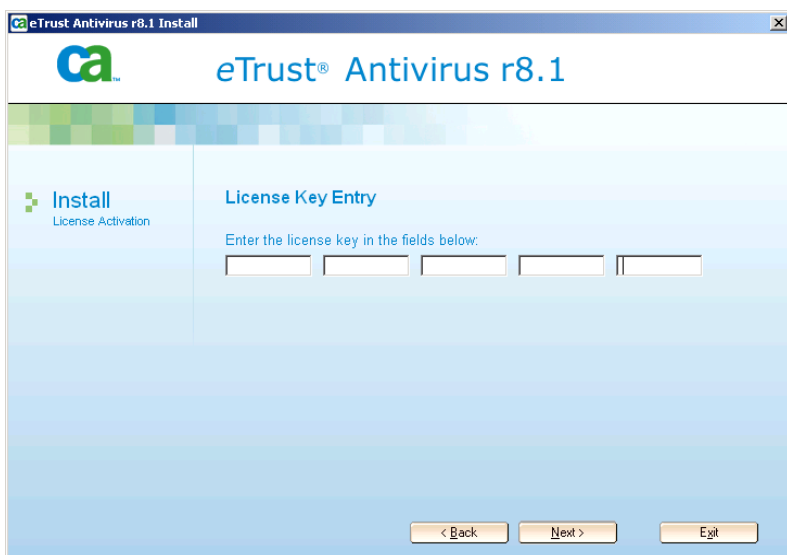


6. Scroll down to read it, and then click **"I agree"**.

7. If, as is recommended by these guidelines, the network is disconnected, just click **"Next >"** for a 30-day trial. Registration will not work while the network is disconnected. We will import a license later in this installation/configuration procedure.



Otherwise, if the network is connected, you can fill in the registration information, click "Next>", then fill in your license key. Note that the key is not validated until the end of the installation. If it is found to be invalid, a 30-day live trial will be installed which you can license later by importing a license.xml file.

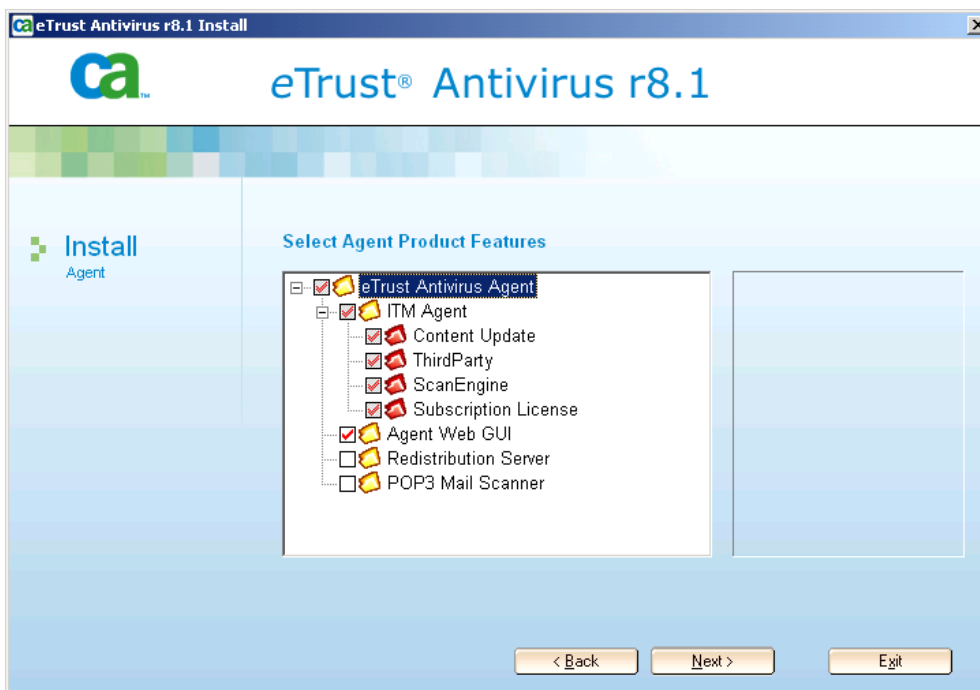


8. Click "**Install eTrust Antivirus r8.1**". Note: If the first selection is "Install eTrust

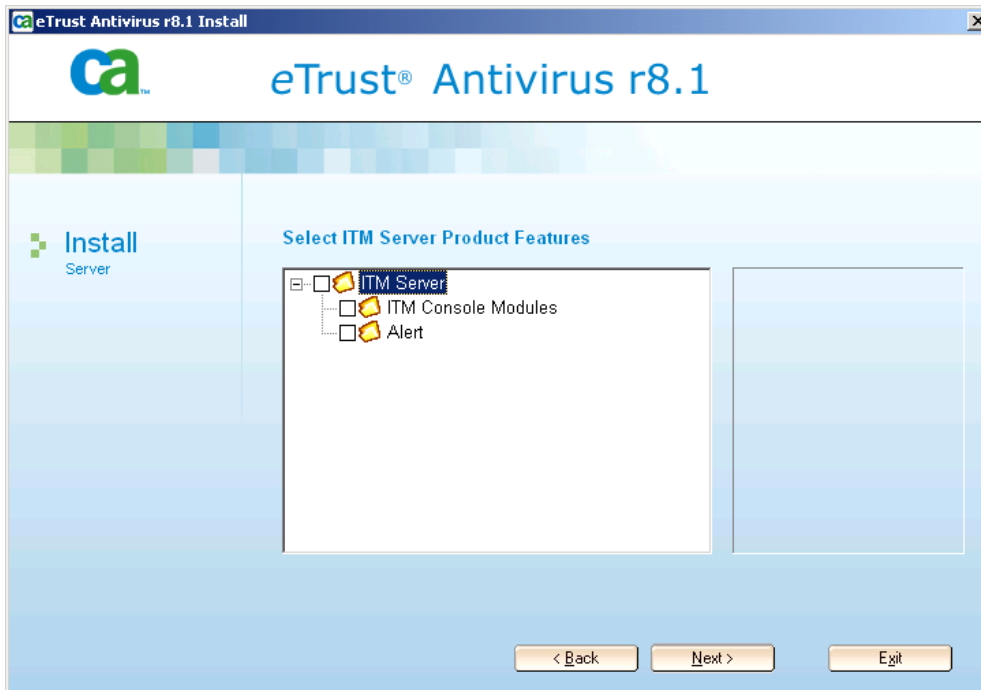
Integrated Threat Management Suite r8.1" instead of "Install eTrust Antivirus r8.1", then you did not properly edit the setup.ini file as described before step 1.



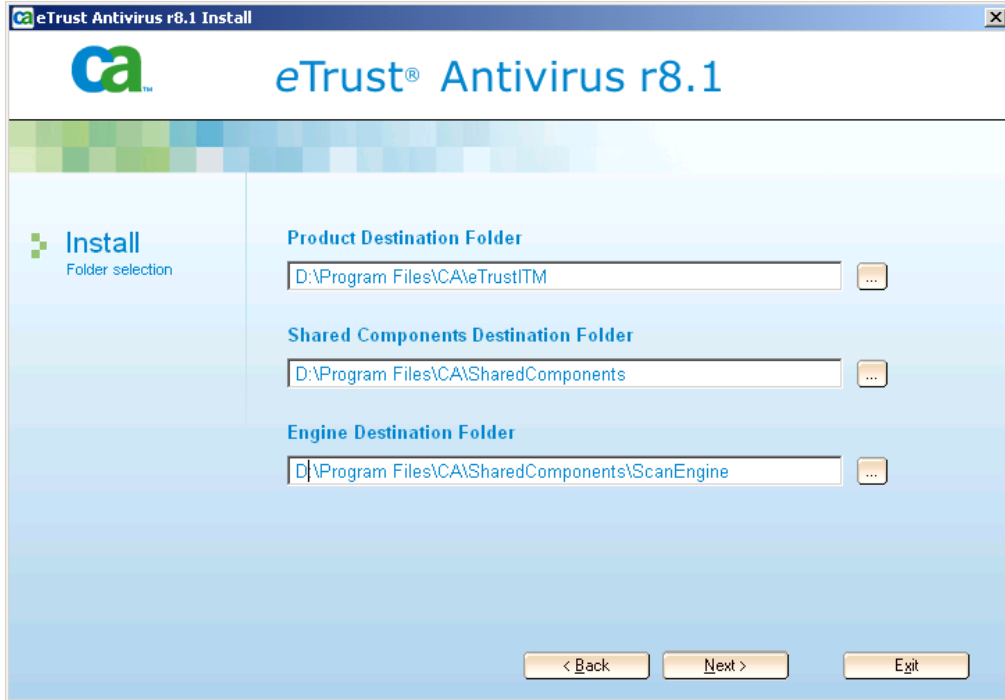
9. Select "**Custom**" and click "**Next >**". Note: Do not install the ITM Server or Redistribution server components on a CallPilot server. Installation of the ITM Server will consume excessive resources and will cause the installation of additional services: Apache Content Server, Apache Tomcat Application Server. This software introduces additional external interfaces that may present security problems.



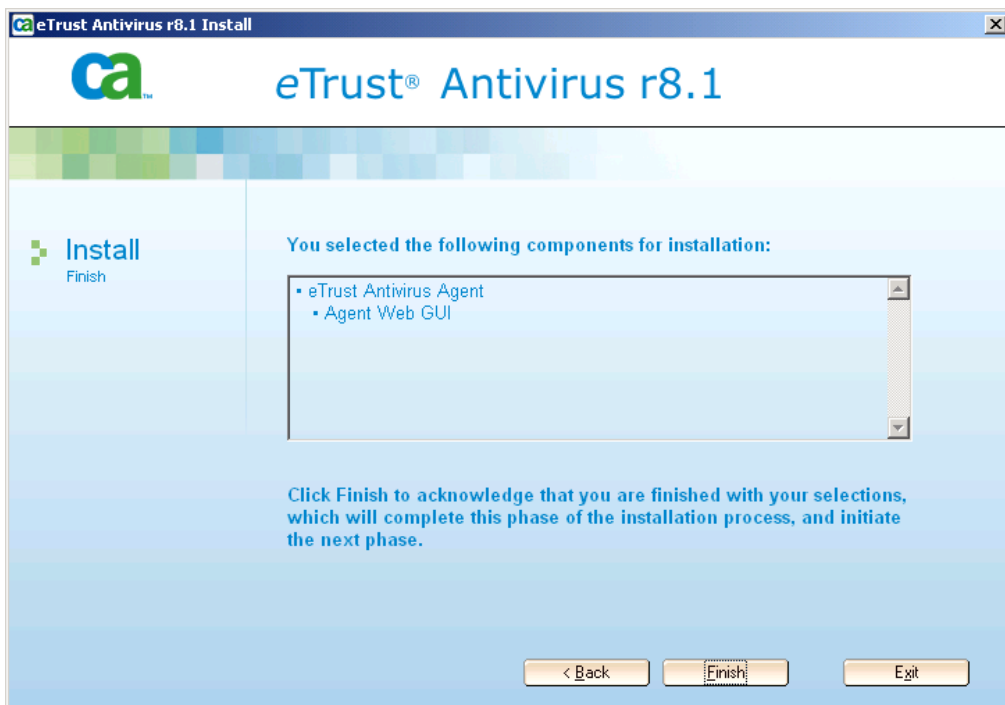
10. Click “**Next >**”



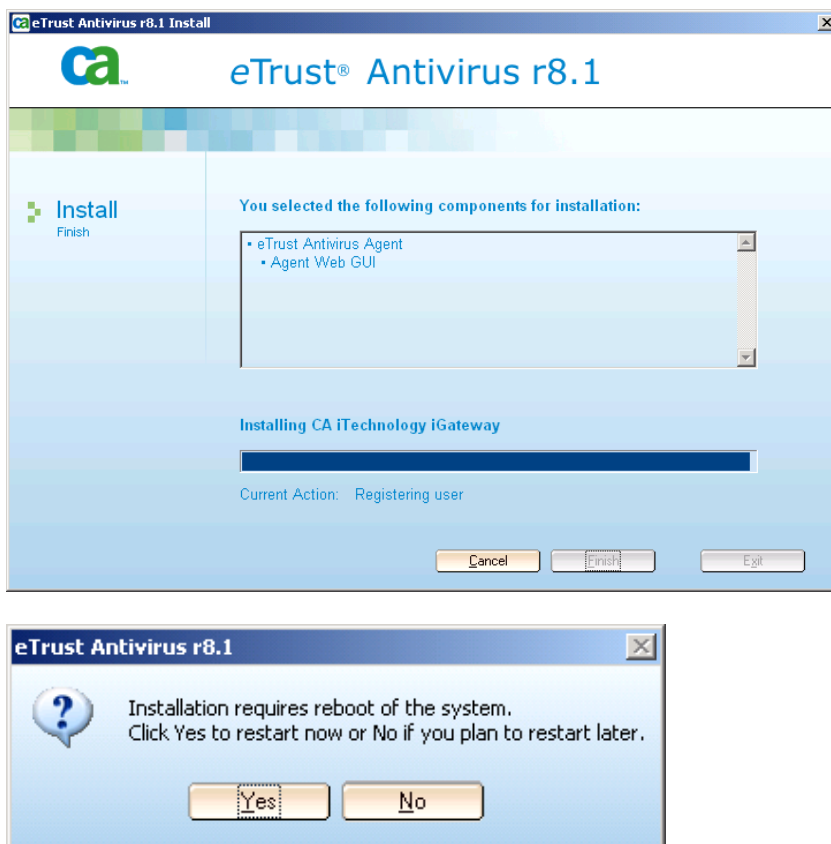
11. Click “**Next >**”. Note: Do not install the ITM Server on a CallPilot server. Installation of the ITM Server will consume excessive resources and will cause the installation of additional services: Apache Content Server, Apache Tomcat Application Server. This software introduces additional external interfaces that may present security problems.



12. On a CallPilot 4.0 system, change the first letter of all three (3) paths to **D:** . For CallPilot 5.0 and later, leave the paths at their default on the **C:** drive. Click "**Next >**".



13. Click "**Finish**". The installation process will proceed as shown.



14. Click “Yes” to reboot. Log back in and wait until server is fully booted up.

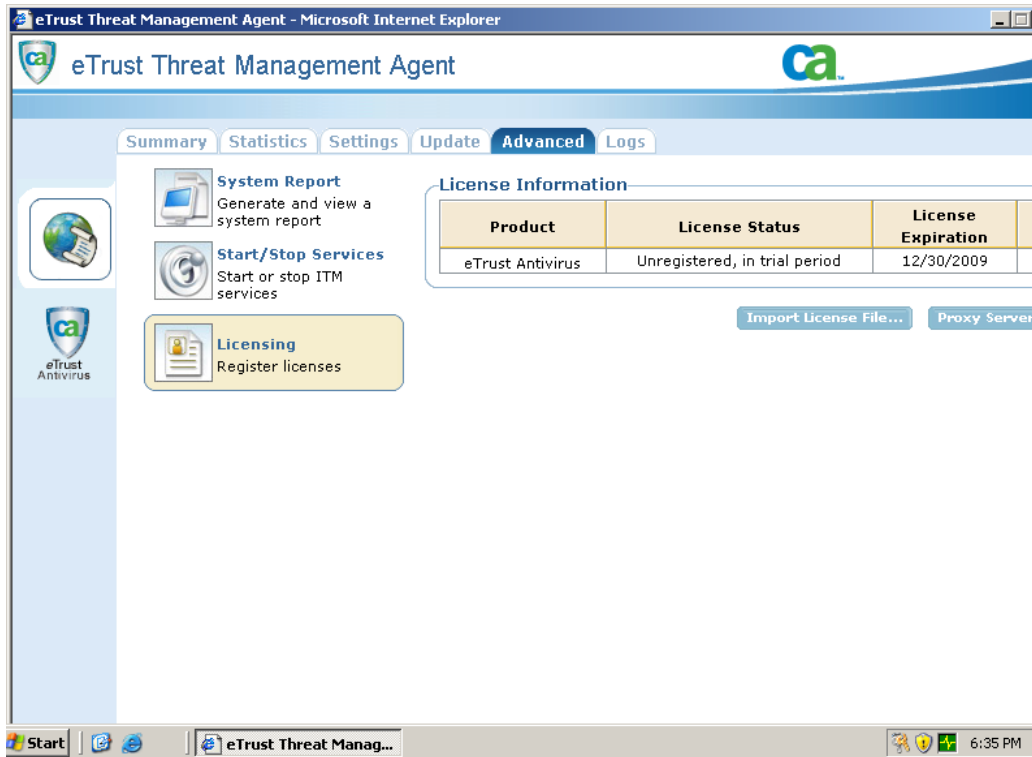
NOTE: After installing eTrust Antivirus 8.1, the Control Panel – Add/Remove Programs List will show two (2) new entries: “CA eTrustITM Agent” and “CA iTechnology iGateway”;. To completely uninstall eTrust Antivirus, it is sufficient to remove only CA eTrustITM Agent.

Avaya recommends that the customer contact CA to obtain any available patches for their eTrust Antivirus 8.1 software. Un-patched bugs in antivirus applications can lead to unexpected problems, including security vulnerabilities in the AV software itself. In particular, there is a reported vulnerability CVE-2009-3587 “CA Anti-Virus vulnerability in the arclib component in the Anti-Virus engine.” The customer is responsible for working with his or her CA support contact to ensure that this and any other known bugs are patched. CA eTrust Antivirus is not an Avaya product and Avaya does not provide product support for this CA product.

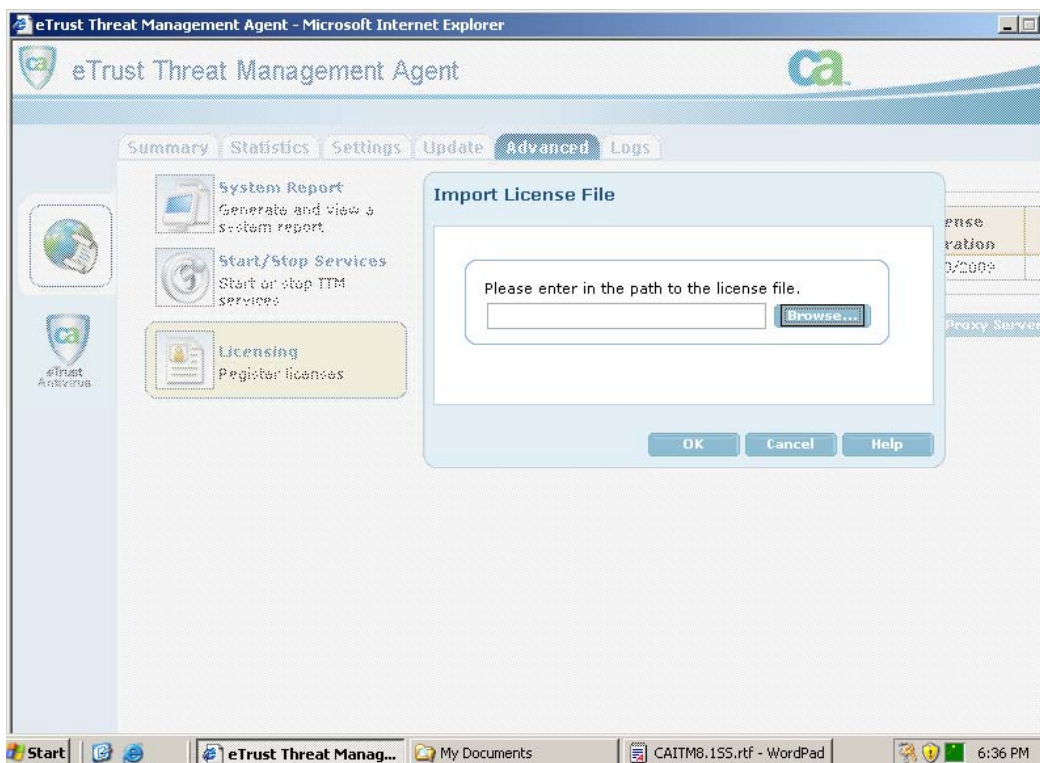
Import a license.xml file

The eTrust Antivirus software must be properly licensed or it will stop working and will be unable to download updated virus definitions. If you did not register and license the software in step 7 above, a license.xml file must be obtained elsewhere (since the ITM Server and Redistribution Server components must never be installed on a CallPilot server), and must be imported into the CA eTrust Antivirus installation on the CallPilot server. Consult the documentation for CA eTrust Antivirus for further information on how to license your CA software. If you have questions about this, contact your CA support representative.

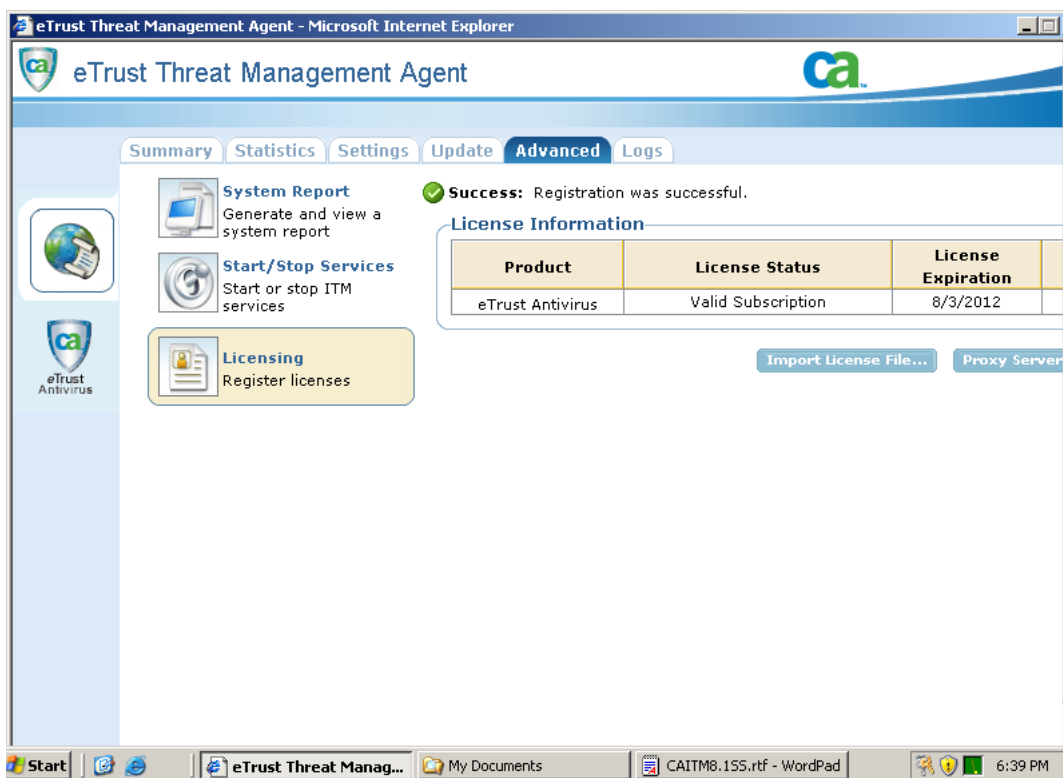
To import a license.xml file, click Start – All Programs – CA – eTrust – eTrustITM – Agent. Select the Advanced tab.



Click “Import license File...”



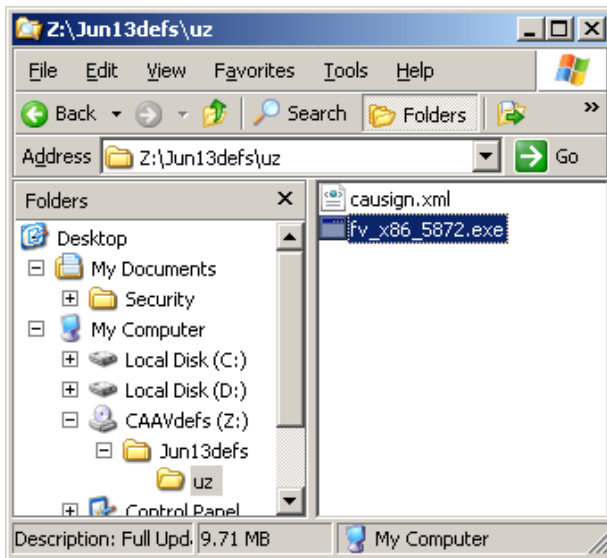
Click **"Browse..."** and navigate to the location of the license.xml file.



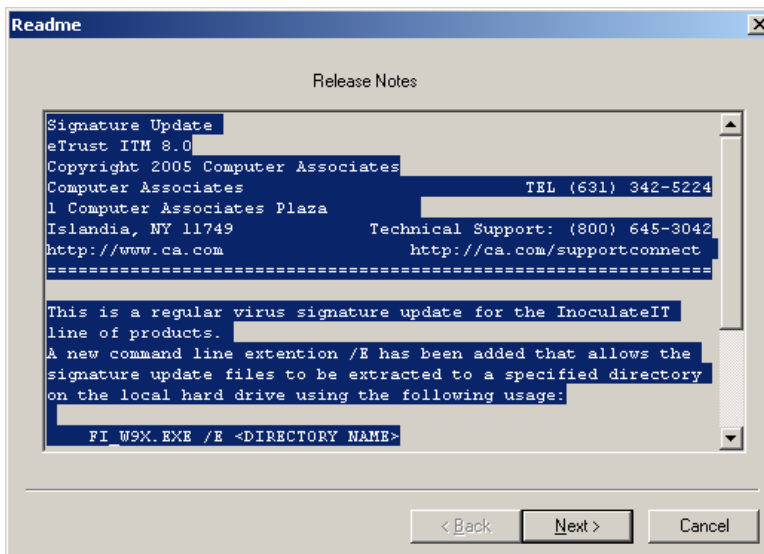
Check the License Expiration date.

Update virus definitions from CD:

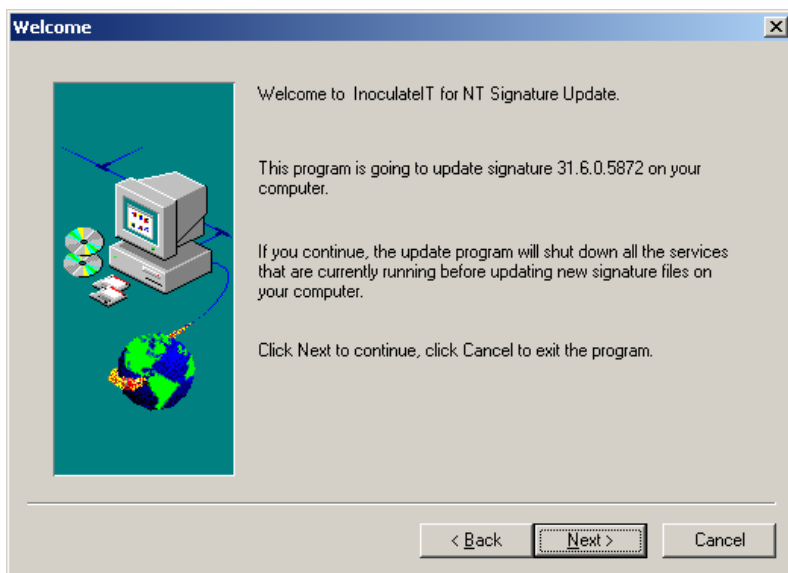
15. Insert CD or USB drive containing previously downloaded definition file. Open Windows Explorer to view it.



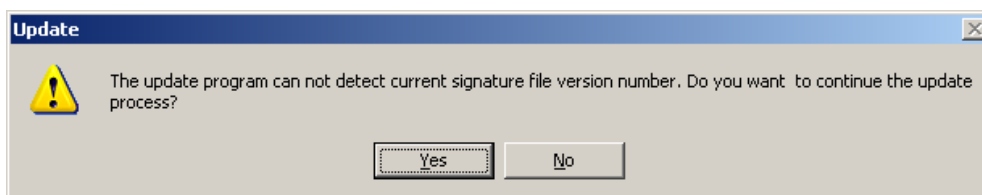
16. Double-click the definition updater “fv_x86_nnnn.exe”.



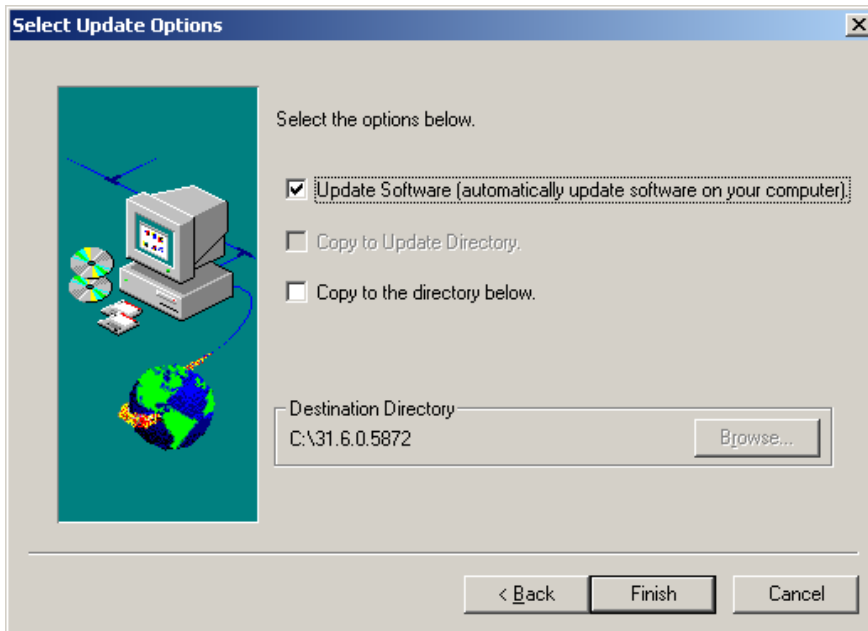
17. Click “Next >”.



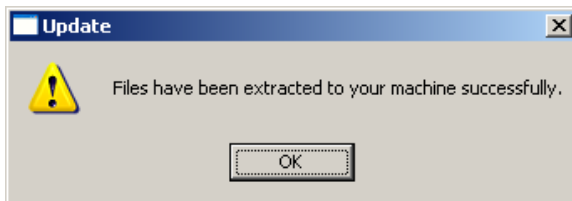
18. Click "**Next >**". You may get the following dialog



19. Click “**Yes**” if the Update dialog appeared, otherwise, go to the next step.



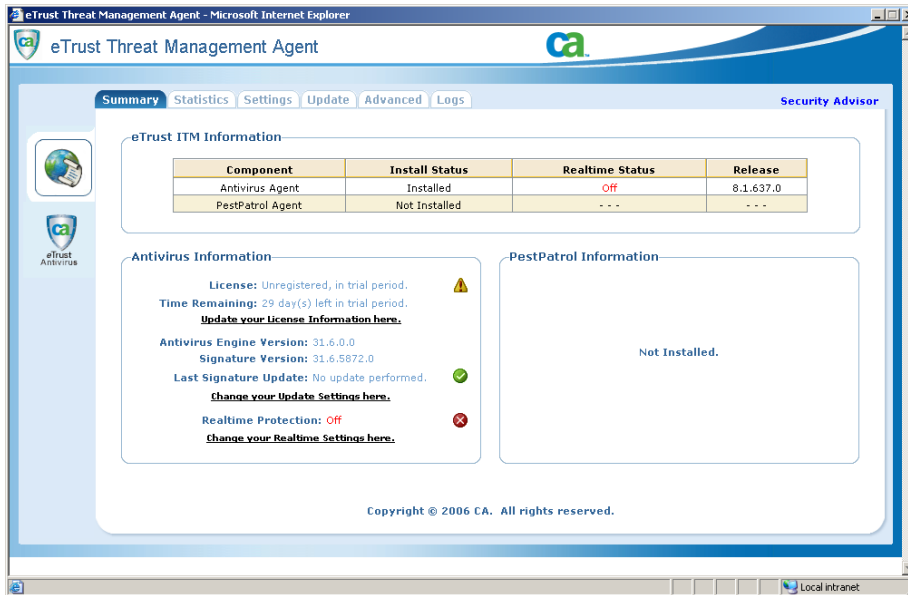
20. Ensure “**Update Software**” is checked, then click “**Finish**”



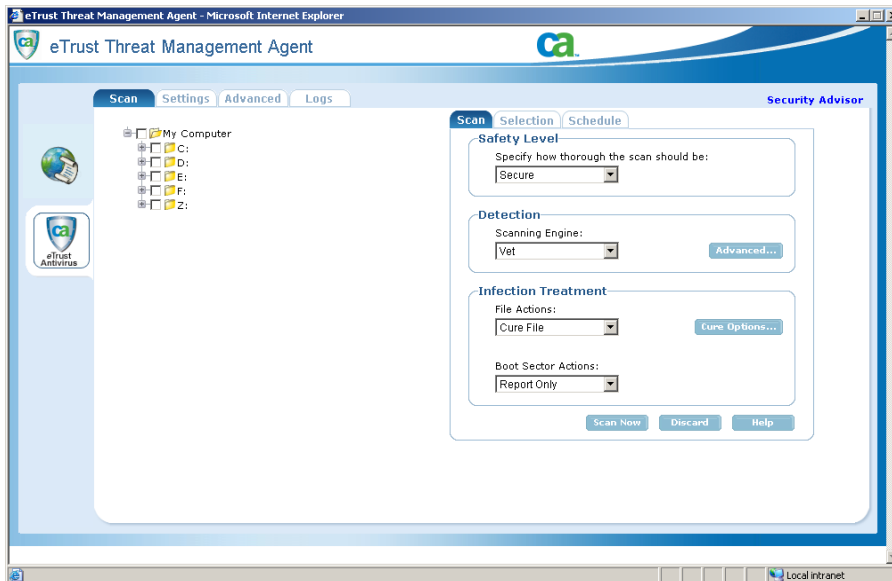
21. Click “**OK**”

Configure CA AntiVirus 8.1

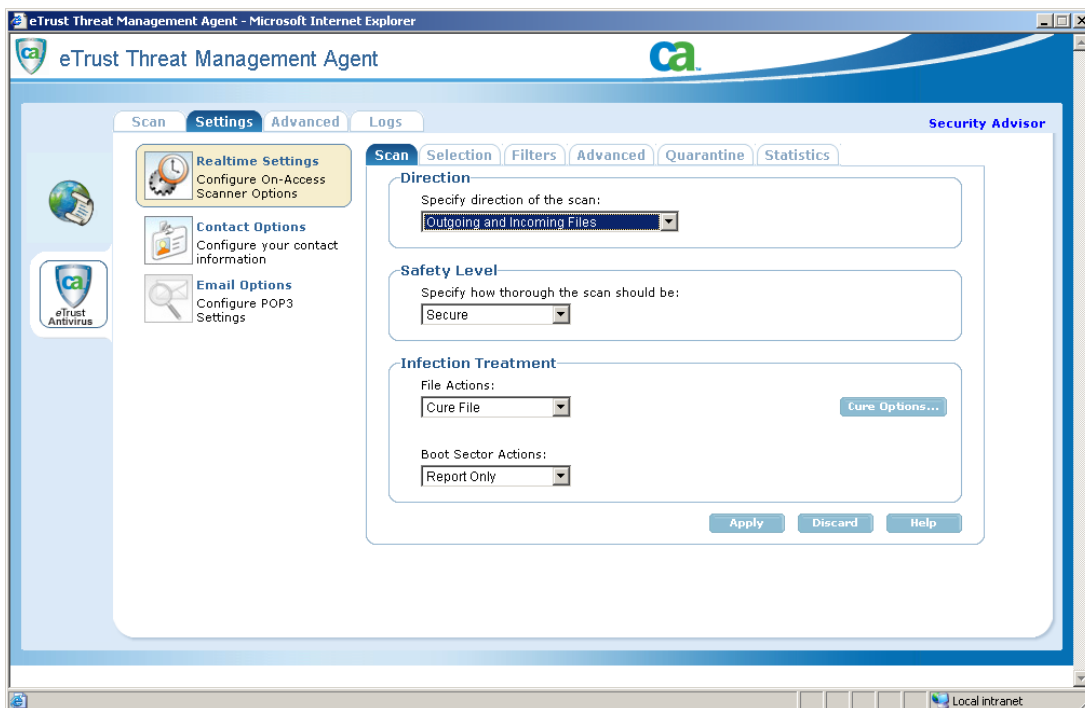
22. Start - Programs - CA - eTrust - eTrustITM – Agent. On the left, select the “**Globe**” Icon.



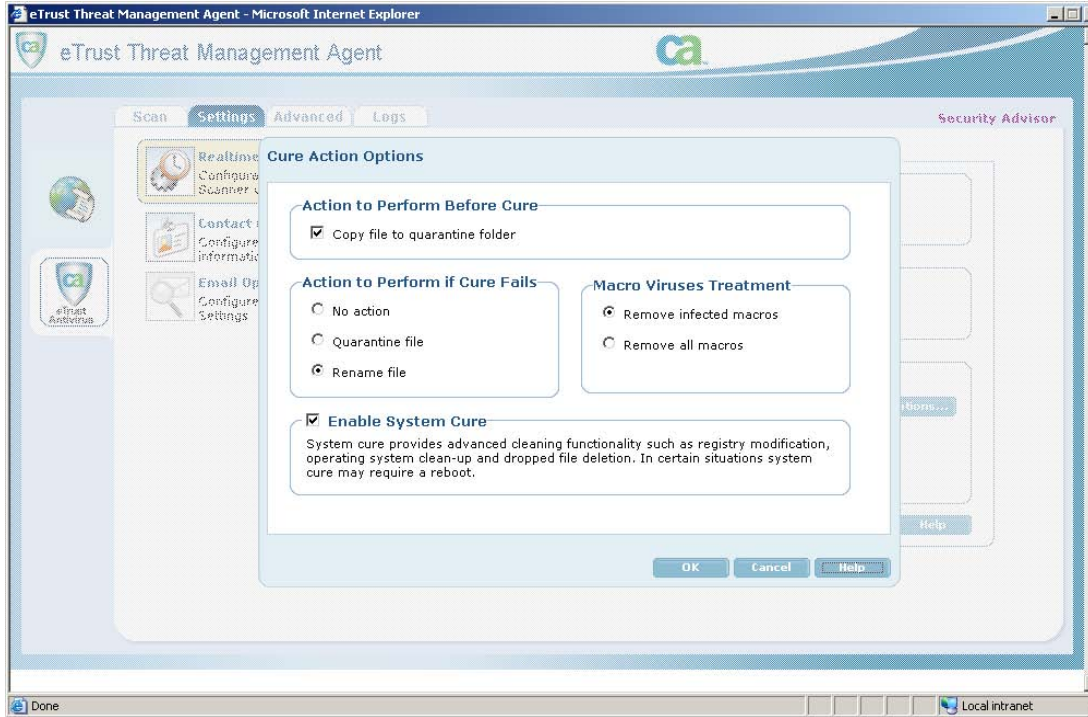
23. Check and confirm the Signature Version number is what you expect. If the screen shows “Realtime Protection” is “Off”, check the tray icon at the right side of the task bar. There should be a “heartbeat” icon. If the icon has a red line through it, hover your mouse over the icon. If it shows “Antivirus: Cannot access Realtime Service”, then you should reboot at this time to ensure that RealTime Protection is operational. Once Realtime Protection is properly enabled, on the left side of the eTrust GUI, click on “**ca eTrust Antivirus**”



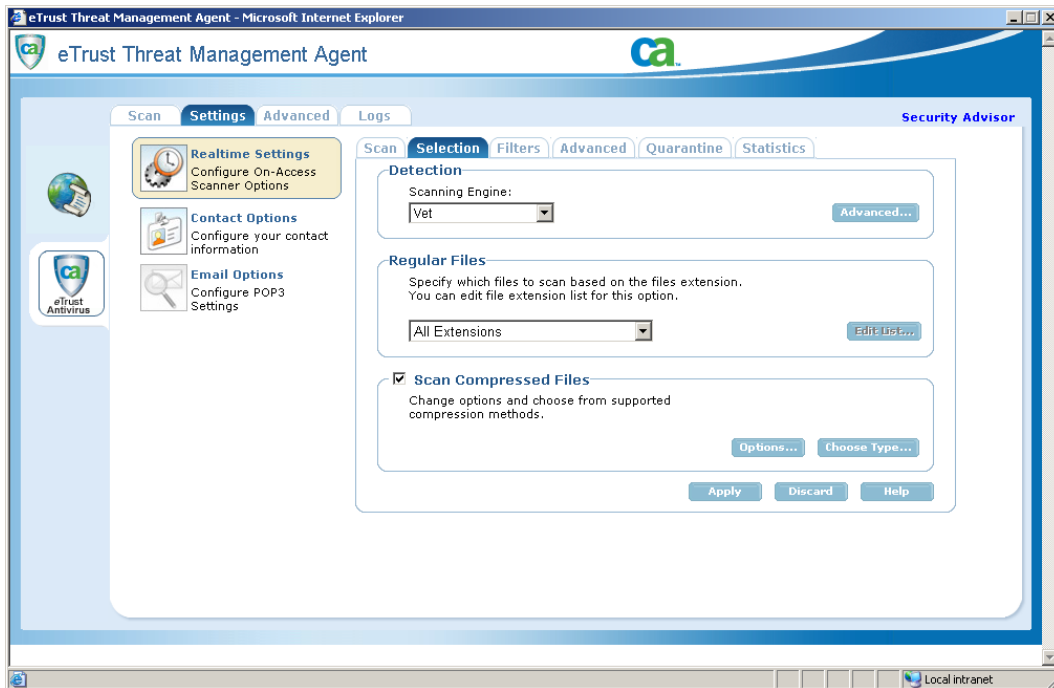
24. Select the **"Settings"** tab



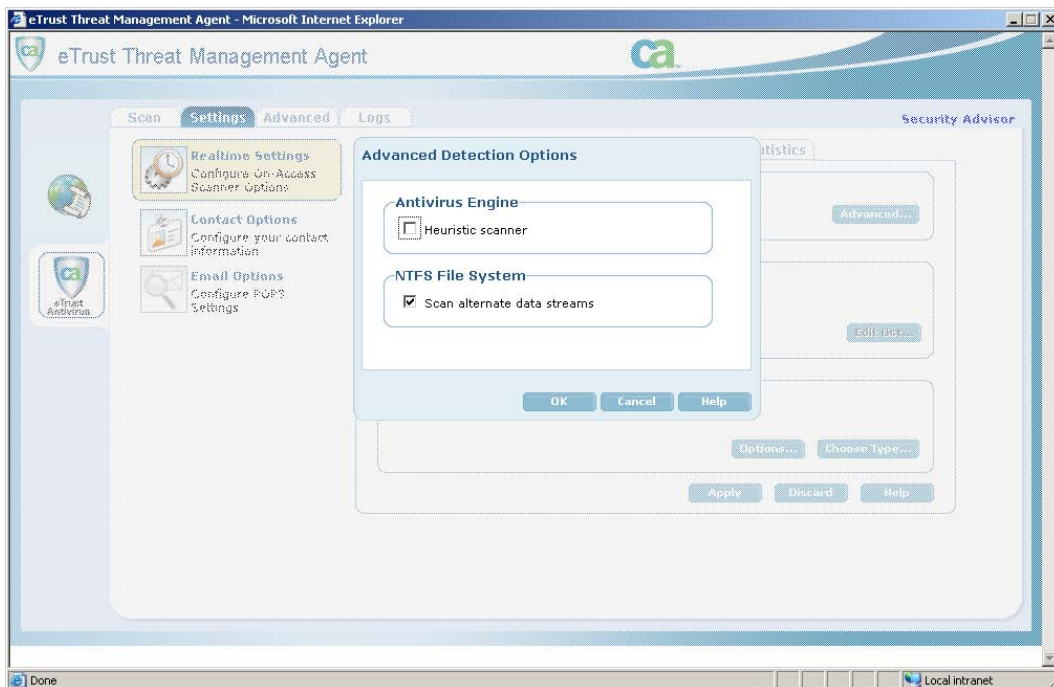
25. On the Scan tab, under Direction, select **"Outgoing and incoming files"**. (Note it is not possible to select incoming only.) Then click **"Cure Options..."**



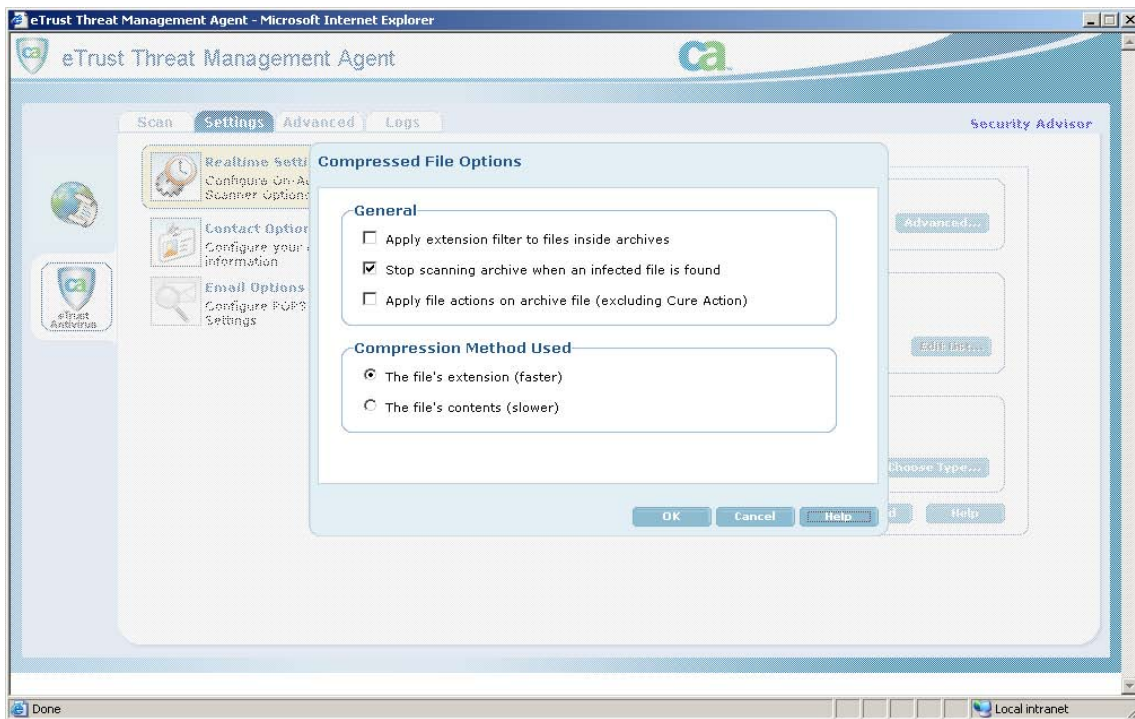
26. Check the box **"Copy file to quarantine folder"**, then click **"OK"**. Then select the **"Selection"** tab



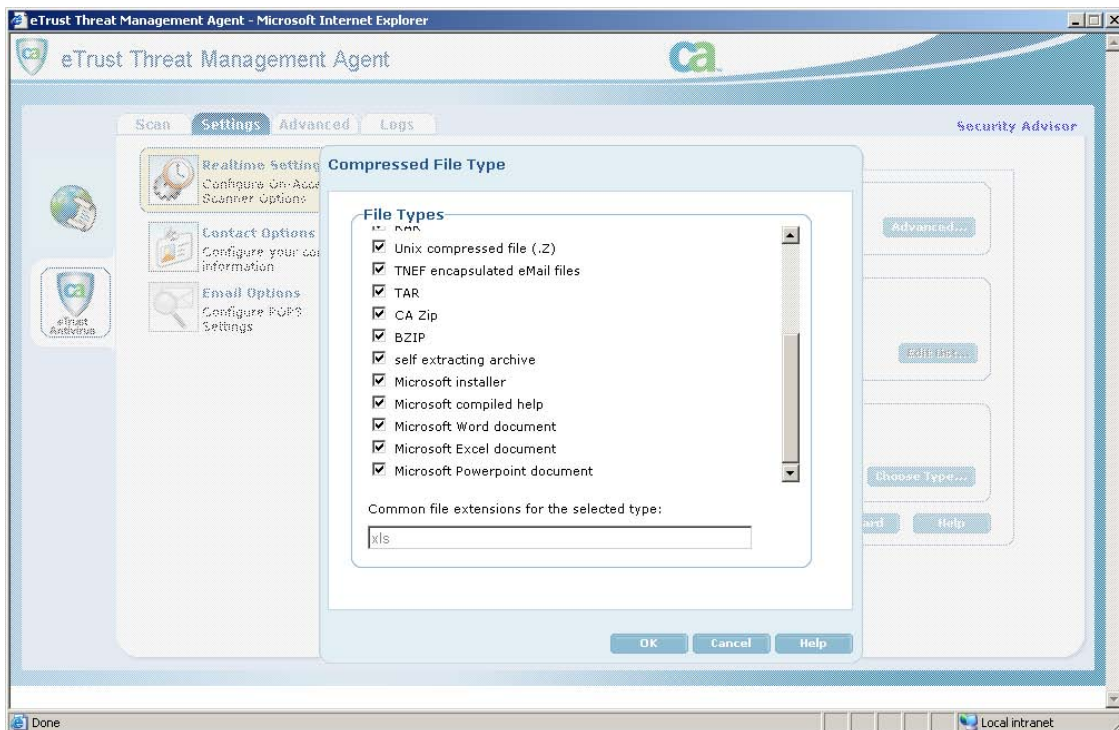
27. Click the **"Advanced"** button and check "Scan alternative data streams". (The Heuristic scanner is too resource intensive so it is not recommended to use it for the Realtime scanning – just the scheduled scans).



28. Click **"OK"**, then click **"Options"** next to "Scan Compressed Files"



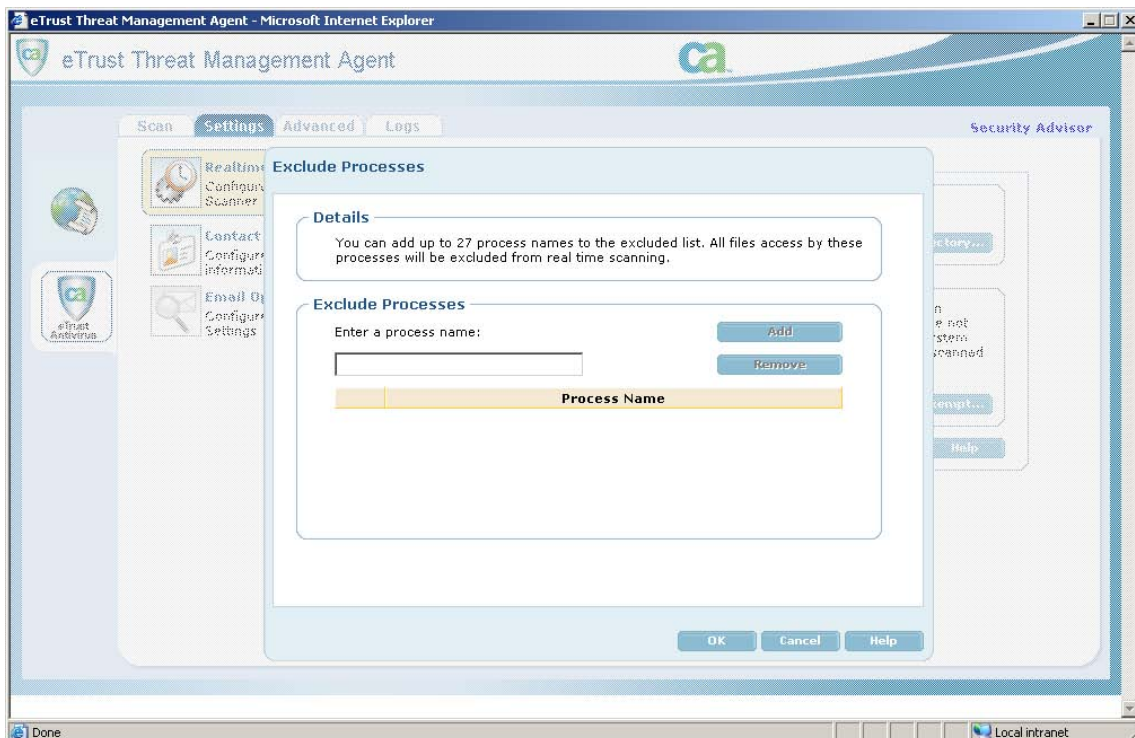
29. No changes are needed on this screen. Click **"OK"**. Click **"Choose Type..."**. Ensure all types are checked (scroll down to see them all)



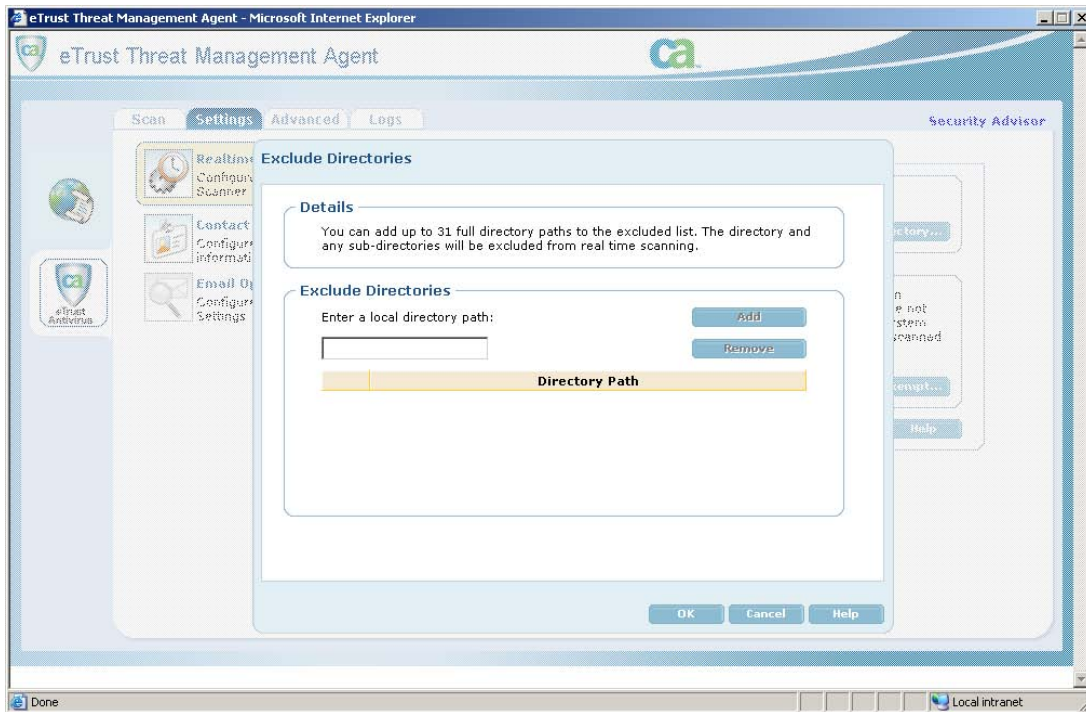
30. Click **"OK"**. Select the **"Filters"** tab.



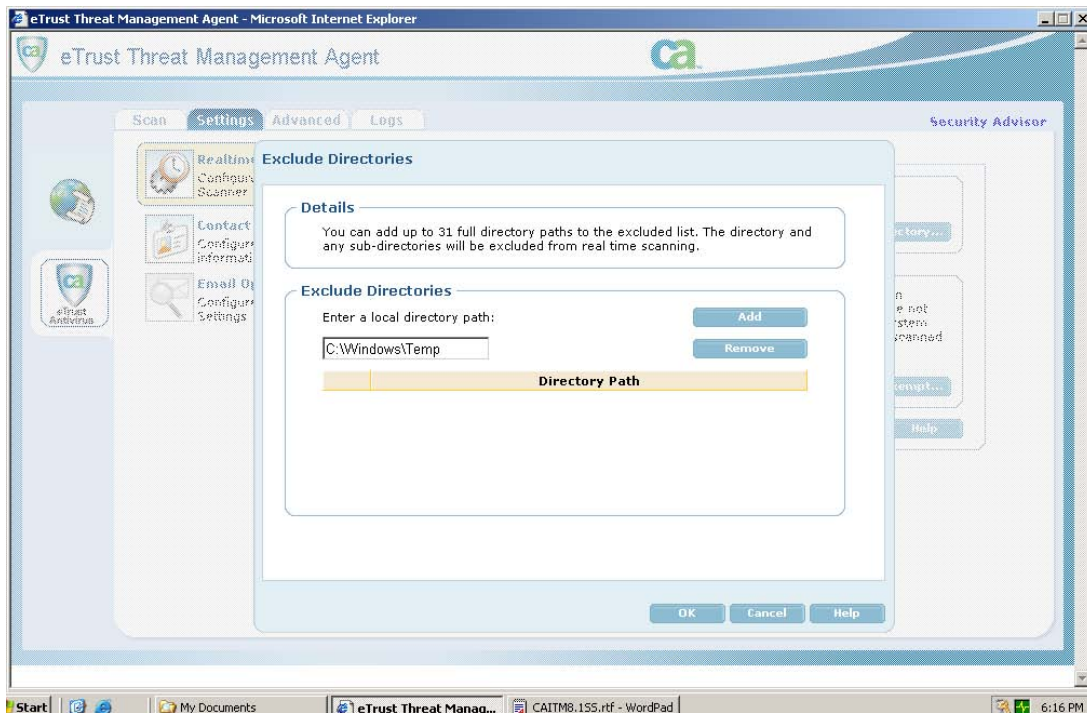
31. Under "Exclusions", click the **"Process..."** button. No changes needed.



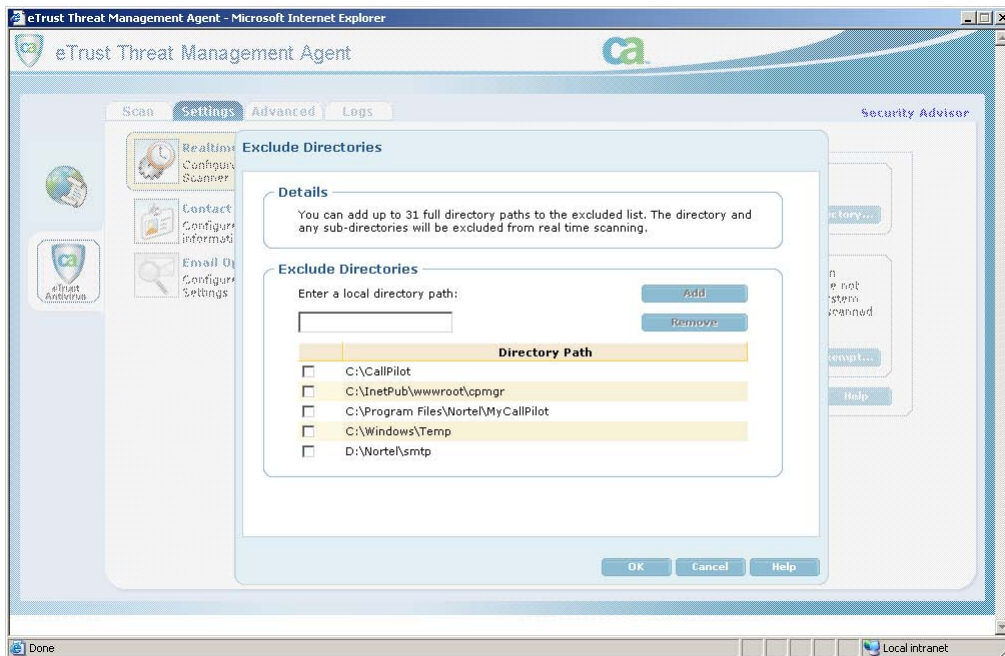
32. Click **“OK”** (no process exclusions set). Under **“Exclusions”**, click the **“Directory...”** button.



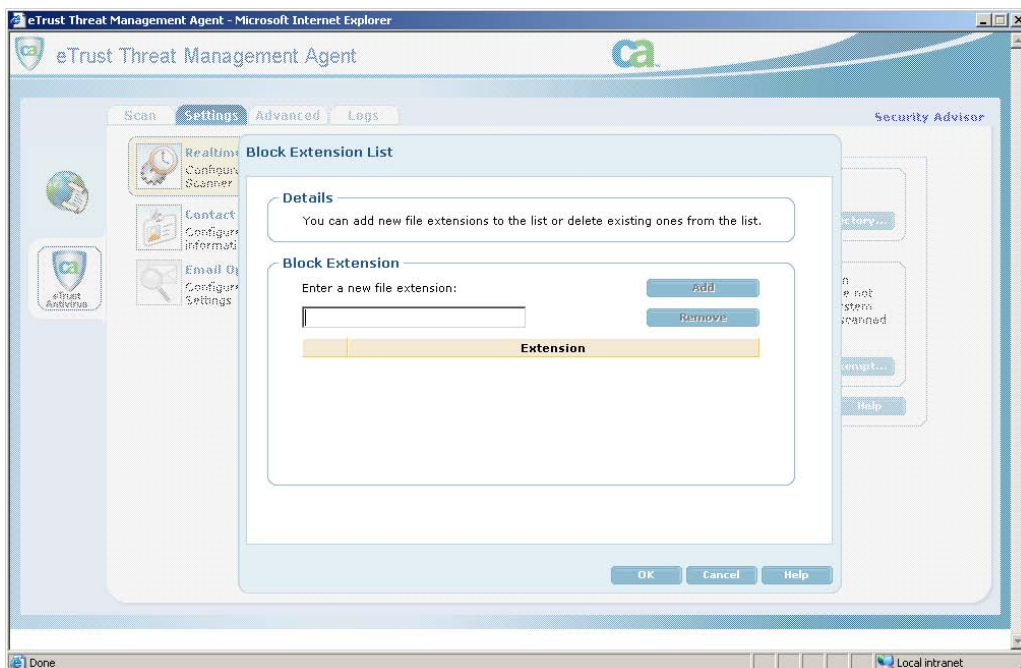
33. Click **“Add”** and type the path **“C:\Windows\Temp”** into the local directory path field.



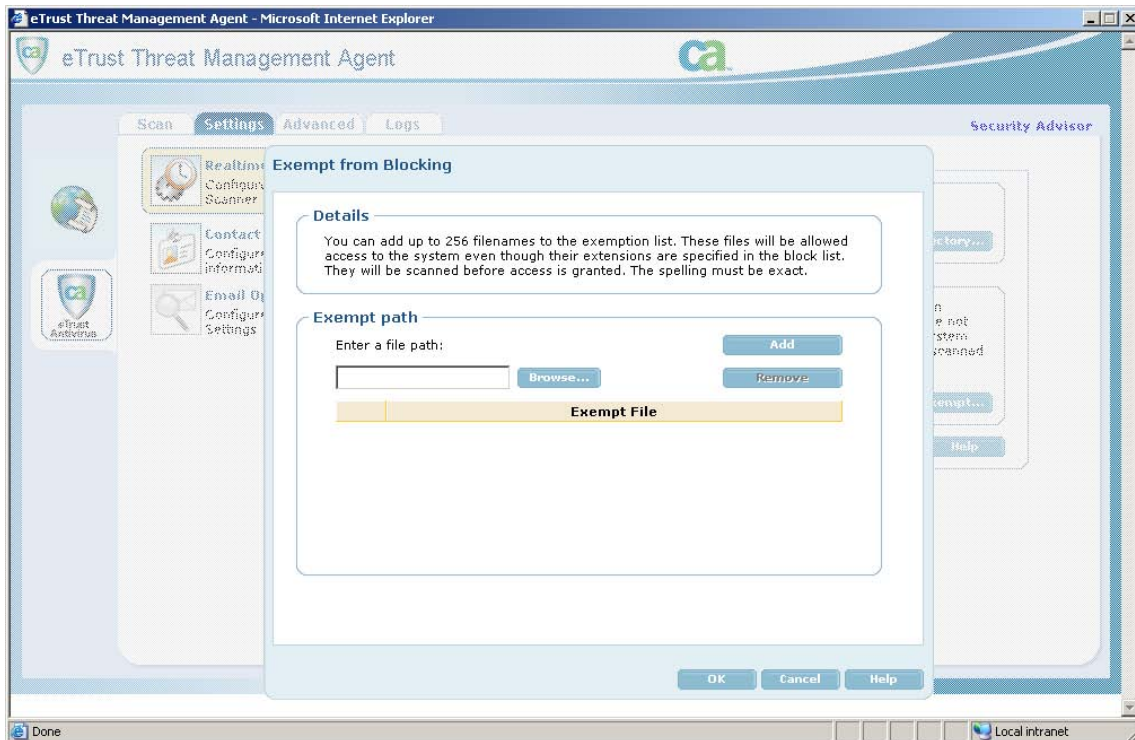
34. Click "Add", then repeat to add all the paths shown below:
- C:\CallPilot
 - C:\InetPub\wwwroot\cpmgr
 - C:\Program Files\Nortel\My CallPilot
 - C:\Windows\Temp
 - D:\Nortel\smtp



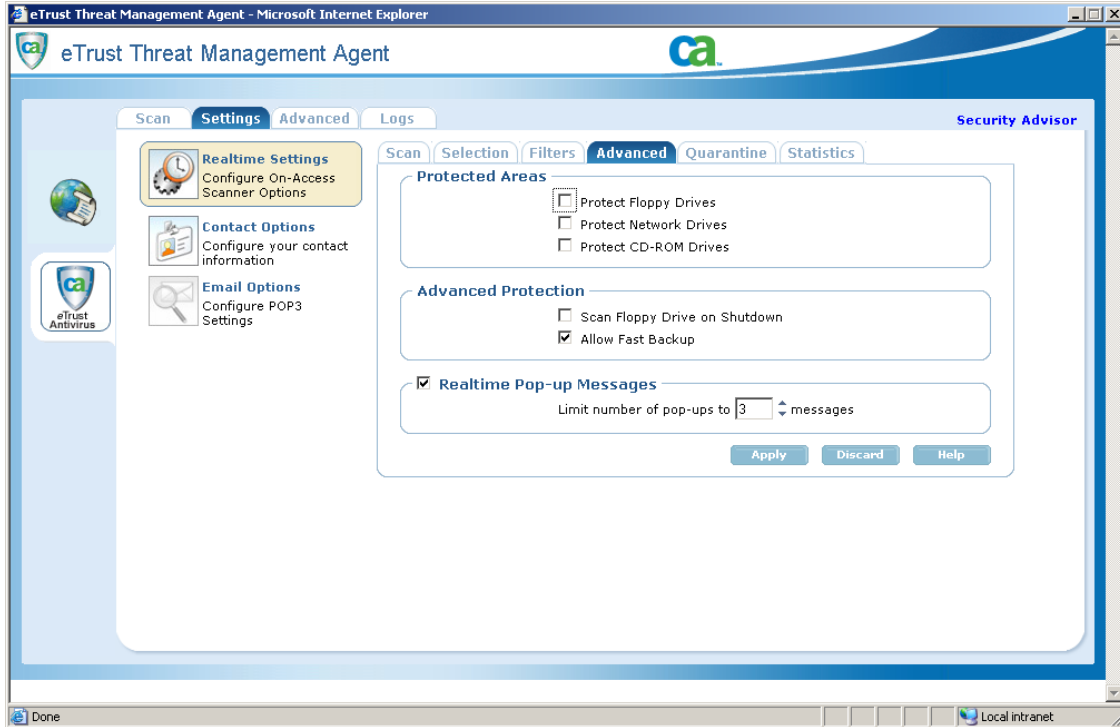
35. Click "OK". Under "Pre-Scan Block" click the "Block..." button.



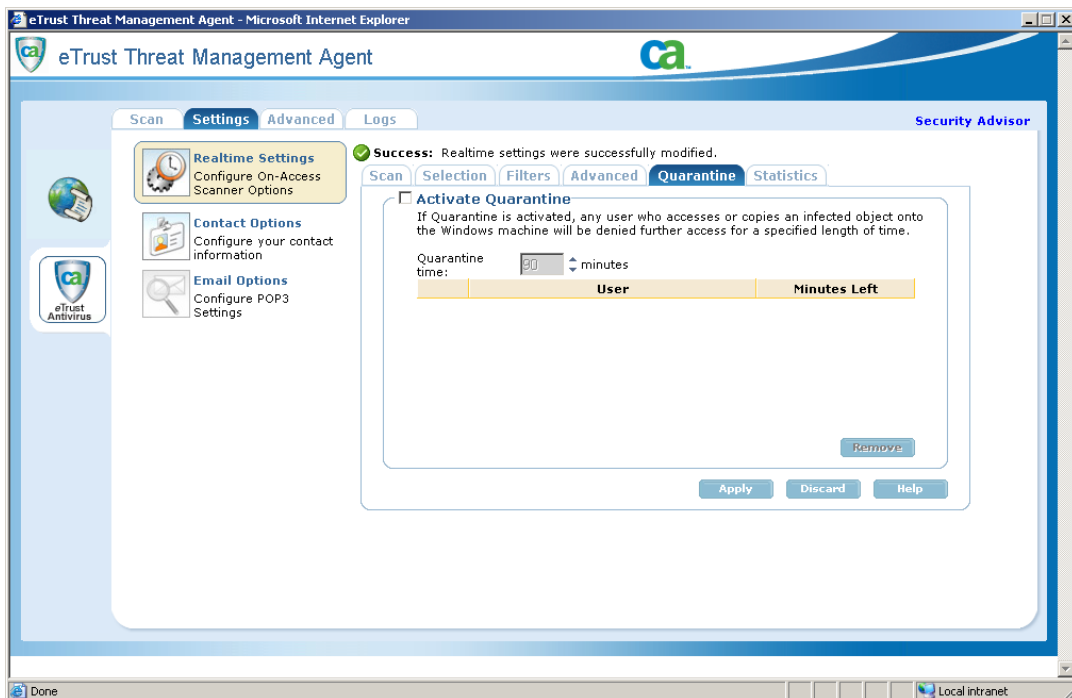
36. Click **"OK"** (no extensions blocked). Click the **"Exempt..."** button



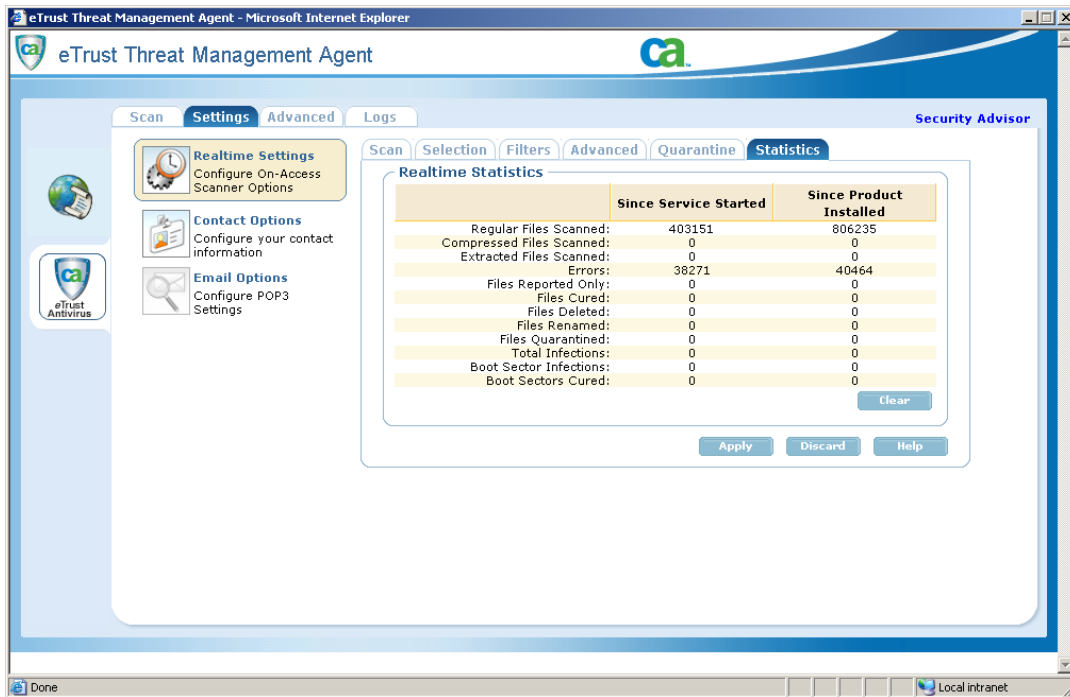
37. Click **"OK"** (no exemptions from blocking defined). Advanced tab. Uncheck **"Protect Floppy Drives"**, and **"Protect Network Drives"**



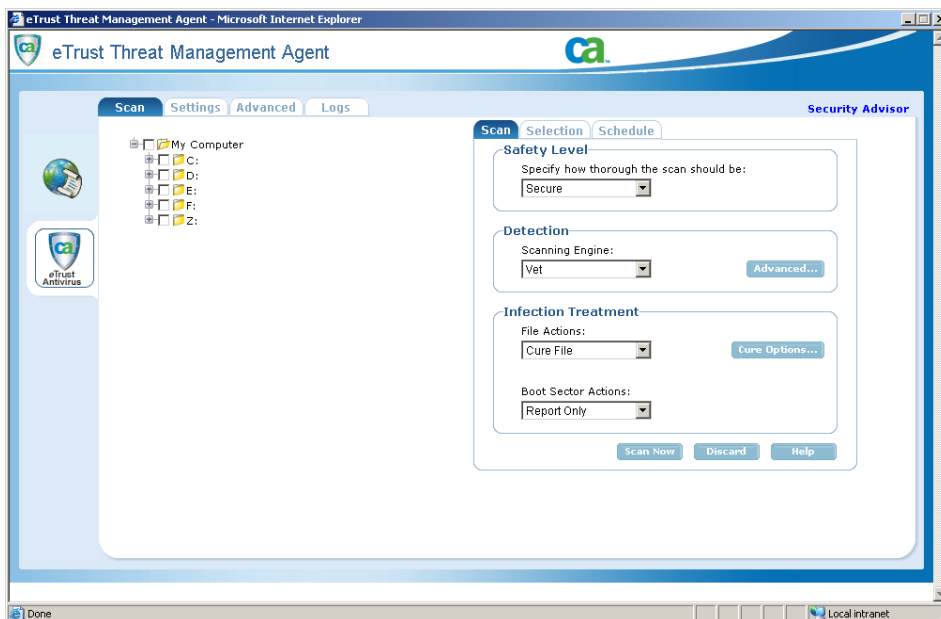
38. Click **“Apply”**. Select the **Quarantine** tab. Do not activate Quarantine. This will block access by a user which accessed an infected file. (This is undesirable since it could prevent access by a needed support person).



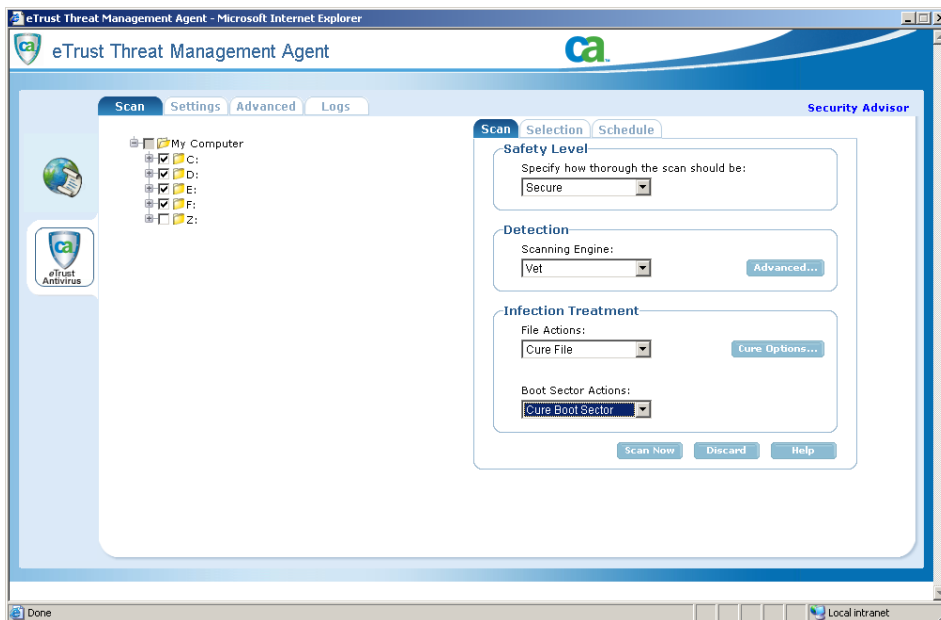
39. Select the **Statistics** tab. This is where statistics for real-time scanning are visible. No need to change anything.



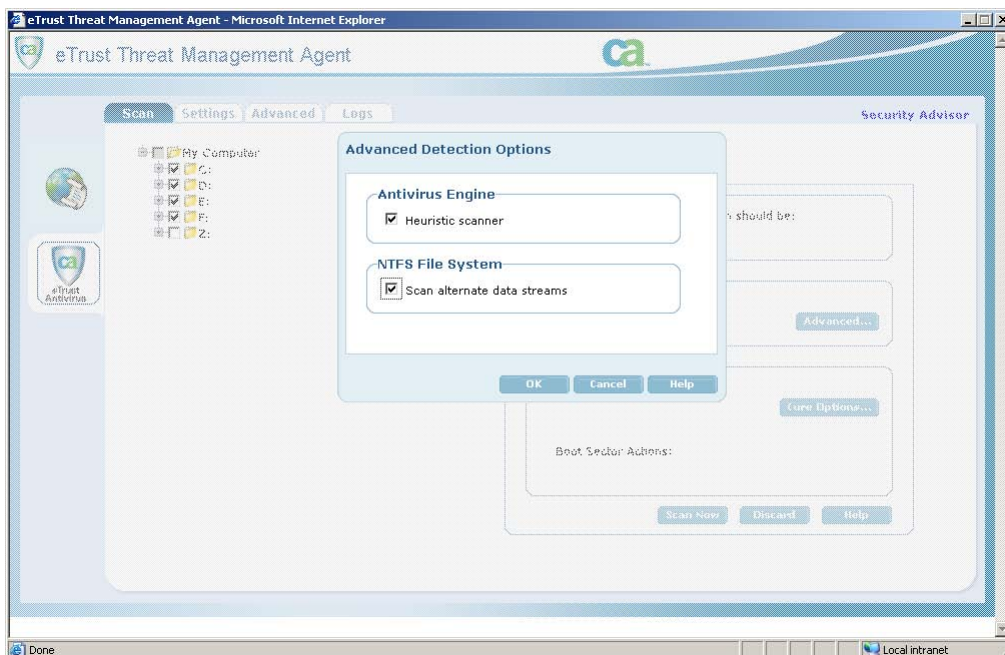
40. Click "Apply" to ensure all real-time settings are saved. At this point, real-time scanning has been configured and virus signatures have been updated so you can reconnect the network cable(s). Then, on the left, select the Scan tab to begin setting up a scheduled full scan.



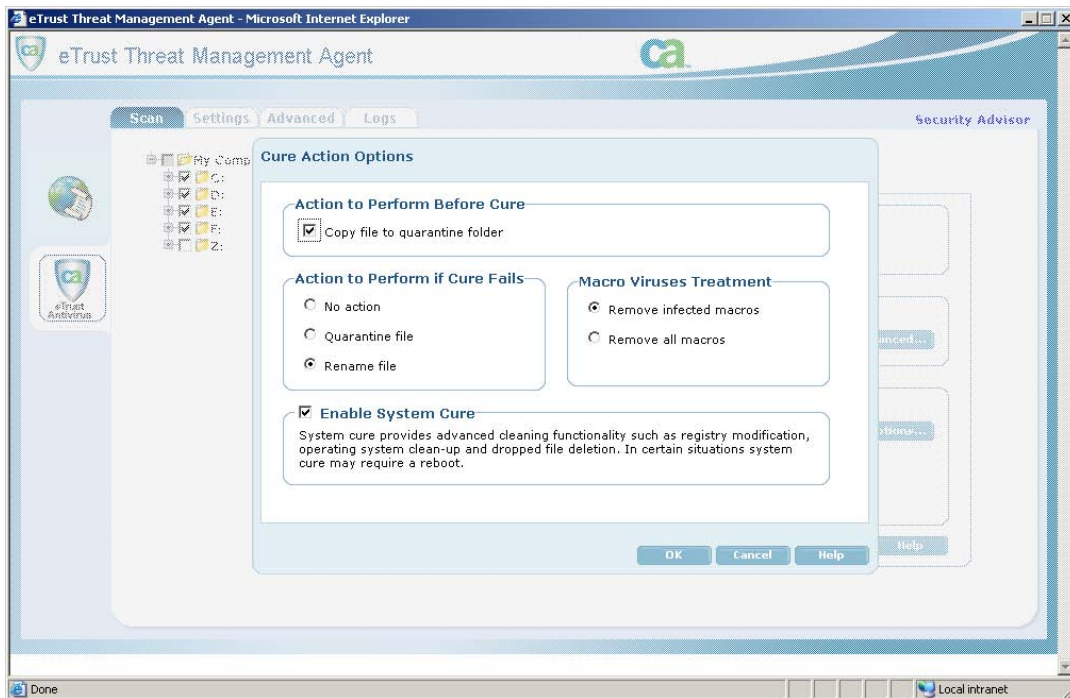
41. Check to select all the hard drives (do not check any floppies, CD drives or USB drives shown – scanning removable media can cause problems if a media error is encountered. All removable media should be checked on a separate, protected workstation prior to being brought to the CallPilot server). Do not select any mapped network drives that may be shown (the CallPilot server should only be responsible for protecting its own disks). Change "**Boot Sector Actions**" to "**Cure Boot Sector**"



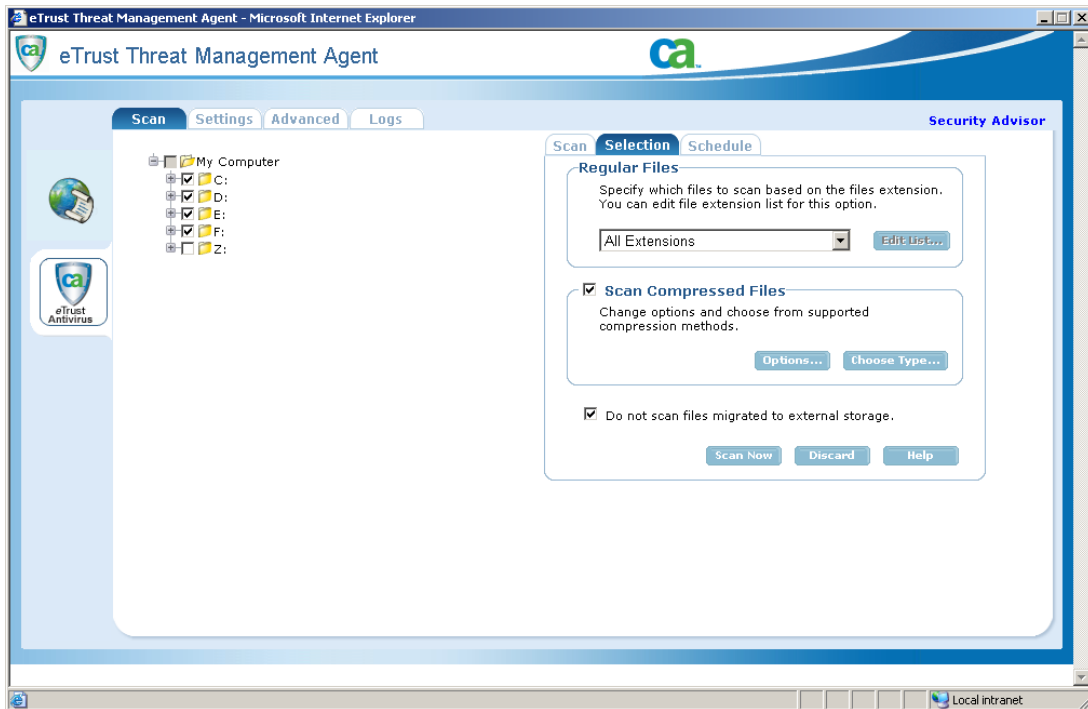
42. Click the **Advanced** button beside the Scanning Engine box. Check **Heuristic scanner** and **Scan alternate data streams**



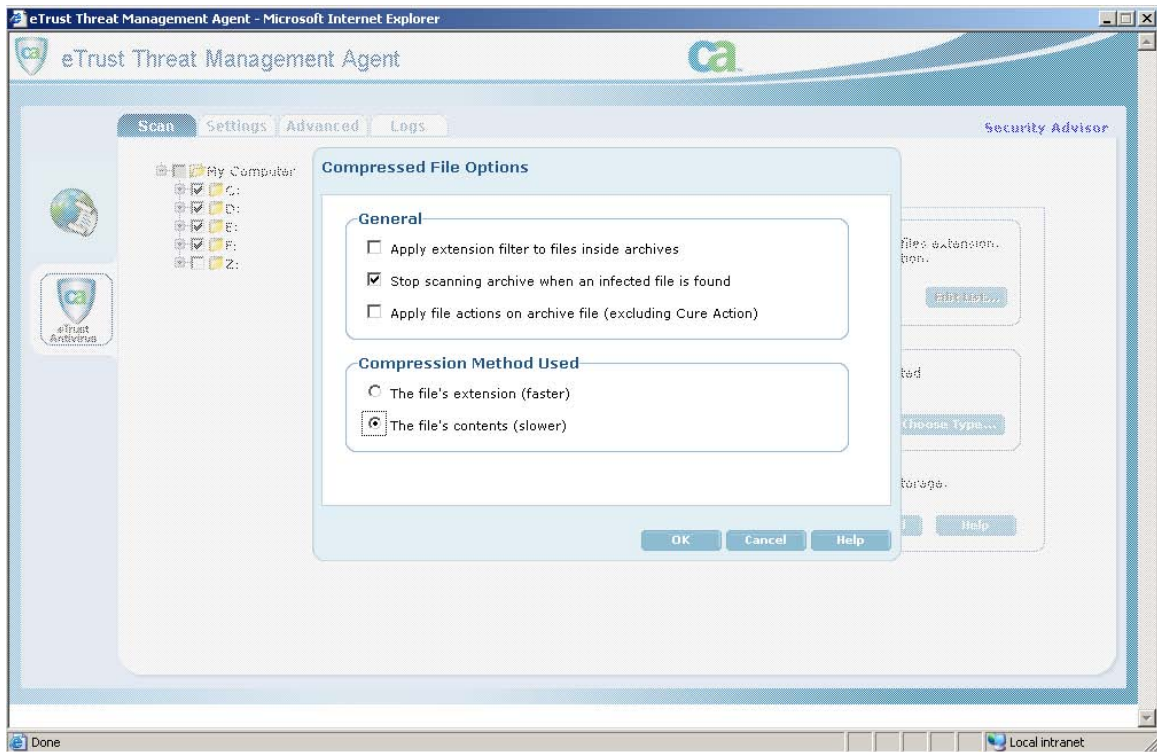
43. Click "OK". Click the "Cure Options" button. Under "Action to Perform Before Cure", check "Copy file to quarantine folder". (Sometimes AV software has "false positives". If the AV software thinks a legitimate file is infected, then we want to be sure we can recover the original file.)



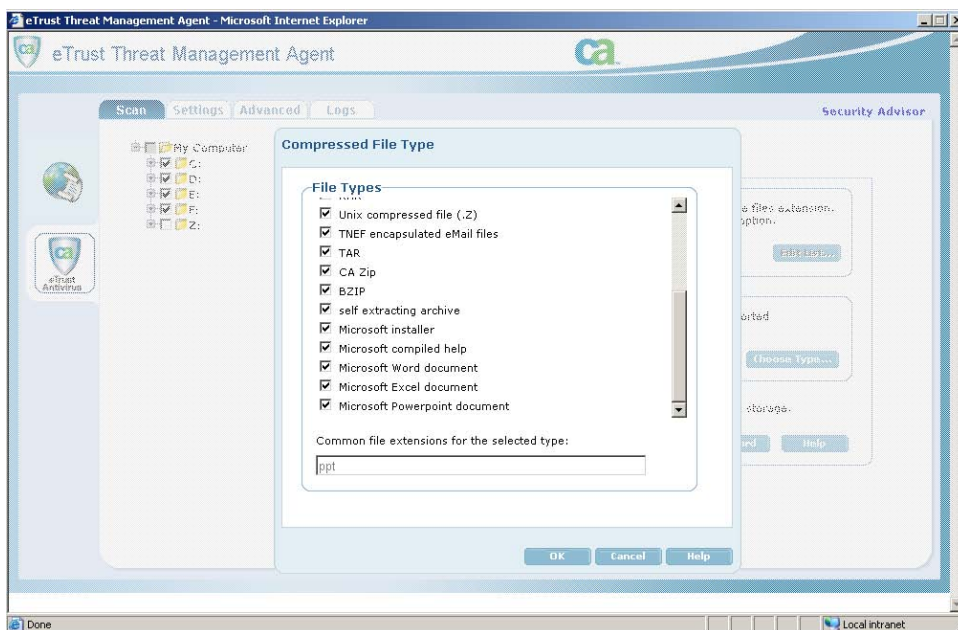
44. Click “OK”. Select the Selection tab



45. Under "Scan Compressed Files" click "**Options...**" Under "Compression Method Used", check "**The file's contents (slower)**"



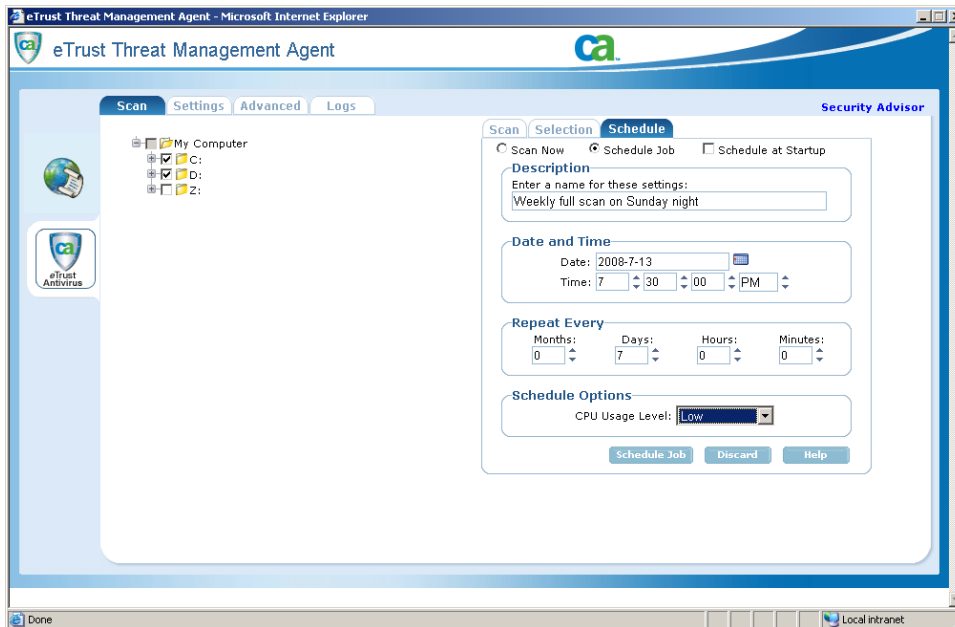
46. Click **“OK”**. Click **“Choose type”** and select all types (scroll down to see them all)



47. Click **“OK”**. Select the "Schedule" tab to schedule a periodic scan of the system.

48. Scanning must be done when the system is expected to be idle or under very low load for the duration of the scan. Select **“Schedule Job”** and enter a meaningful name for the

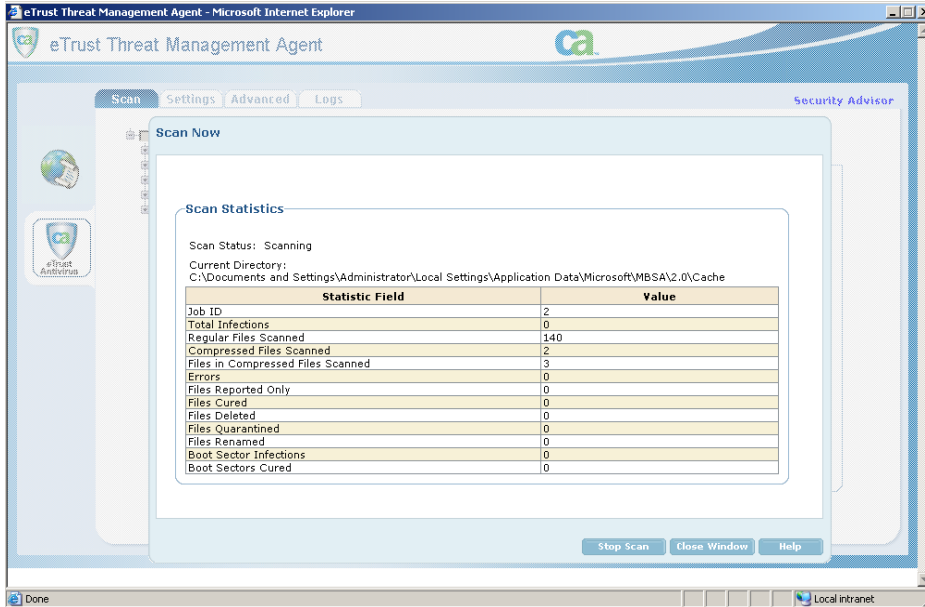
scan. If you want to set up a weekly scan, use the calendar button to pick an appropriate date for the first scan. Pick a time when the system is expected to have very low load for the several hours needed to do the scan. For a weekly scan, set the "Repeat Every" value to seven (7) days. Set the CPU usage level to low to minimize system impact during the scan.



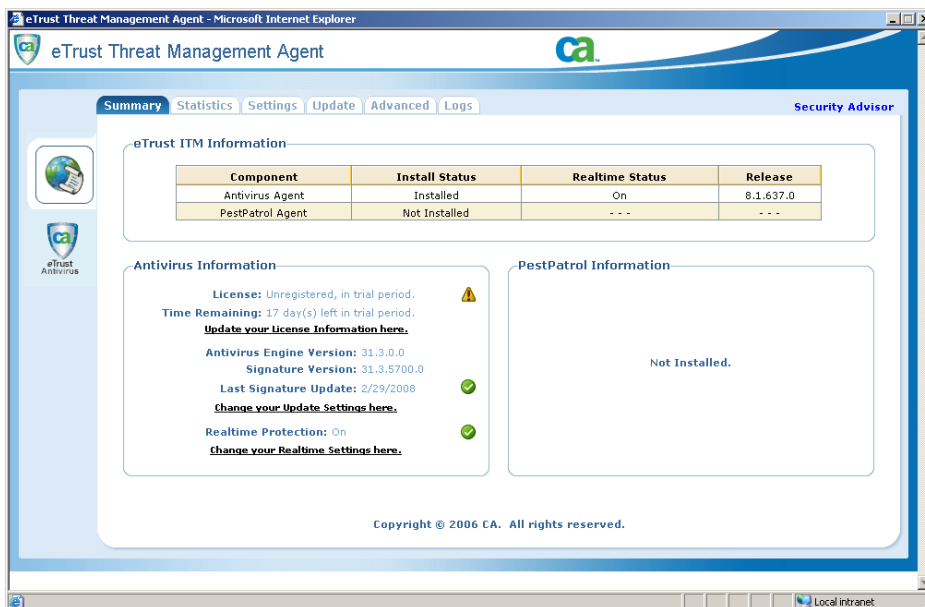
49. Click "**Schedule Job**" to save the scheduled scan.

50. To check all created scan jobs, select "Advanced" tab, then "Job Queue"

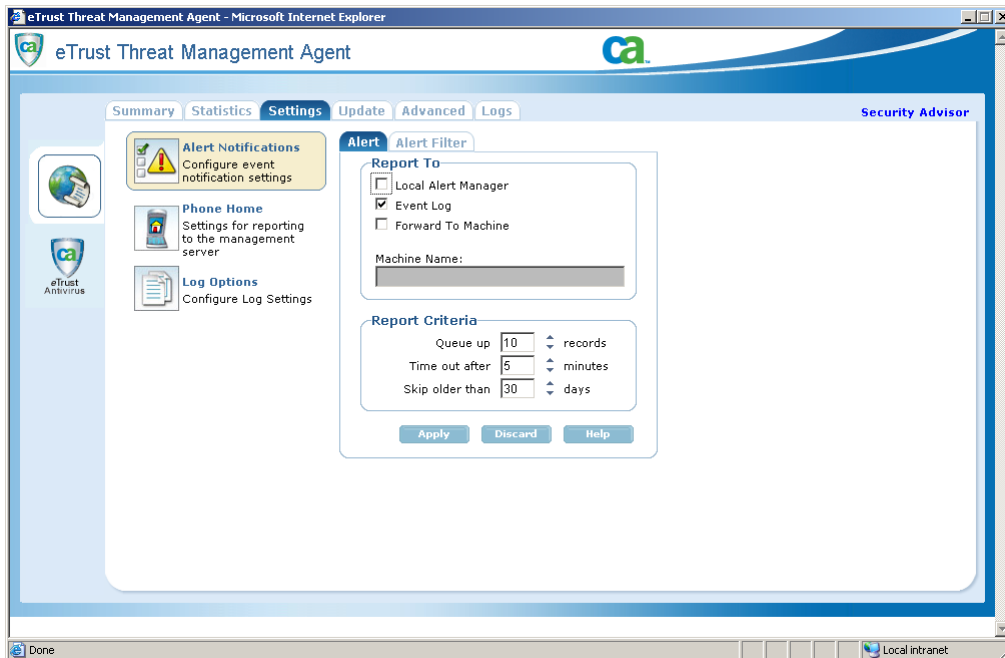
51. To ensure the system has no pre-existing infection, you may want to perform a full scan now. (Skip this step if you are confident the system has no existing infections.) Select all hard drive letters and click "**Scan Now**". You may want to set the detailed scan parameters by following steps 41 to 48 above. The scan will take 90 minutes or more to complete on a 201i server (less on a faster server). Wait until done.



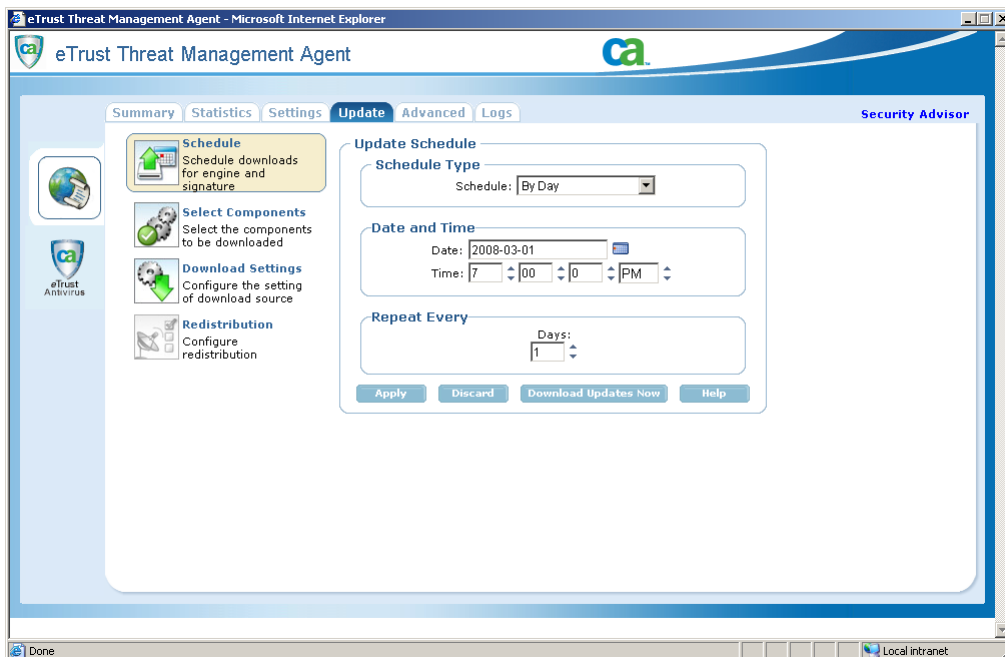
52. At the left of the window, click on the "globe" icon



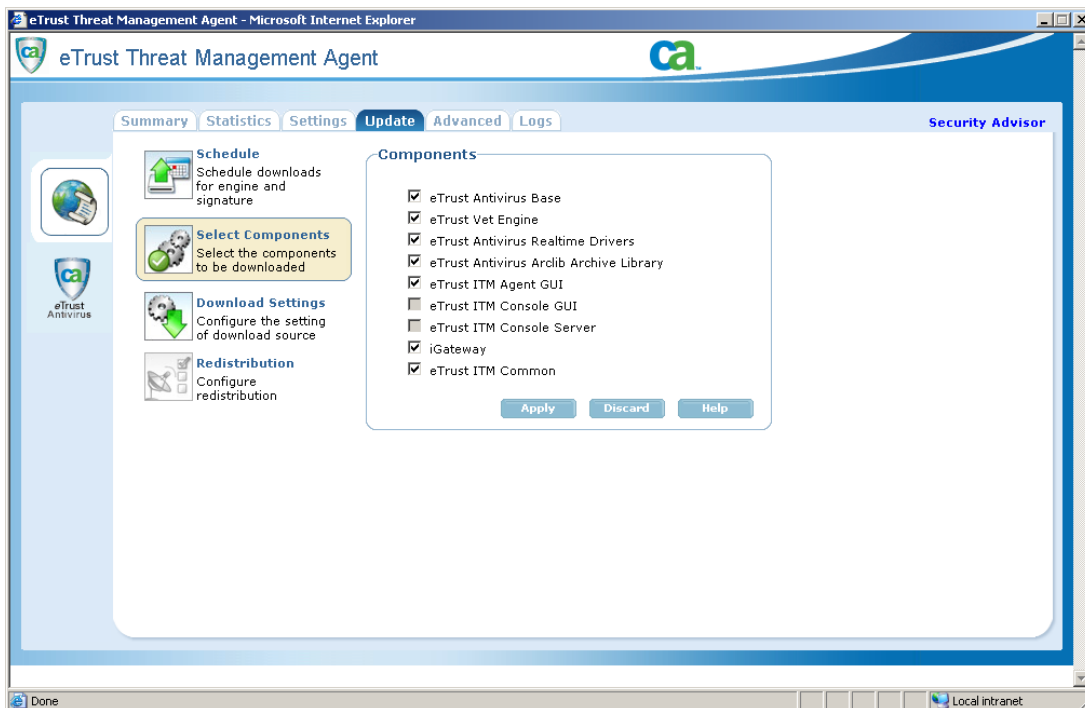
53. Select the Settings tab. On the "Alert" tab, under "Report to", check "**Event Log**" and click "**Apply**". You may also want to set up "Forward to Machine". (The Local Alert Manager has not been installed on the CallPilot server). You can also set up "Phone Home" and "Log Options" if desired.



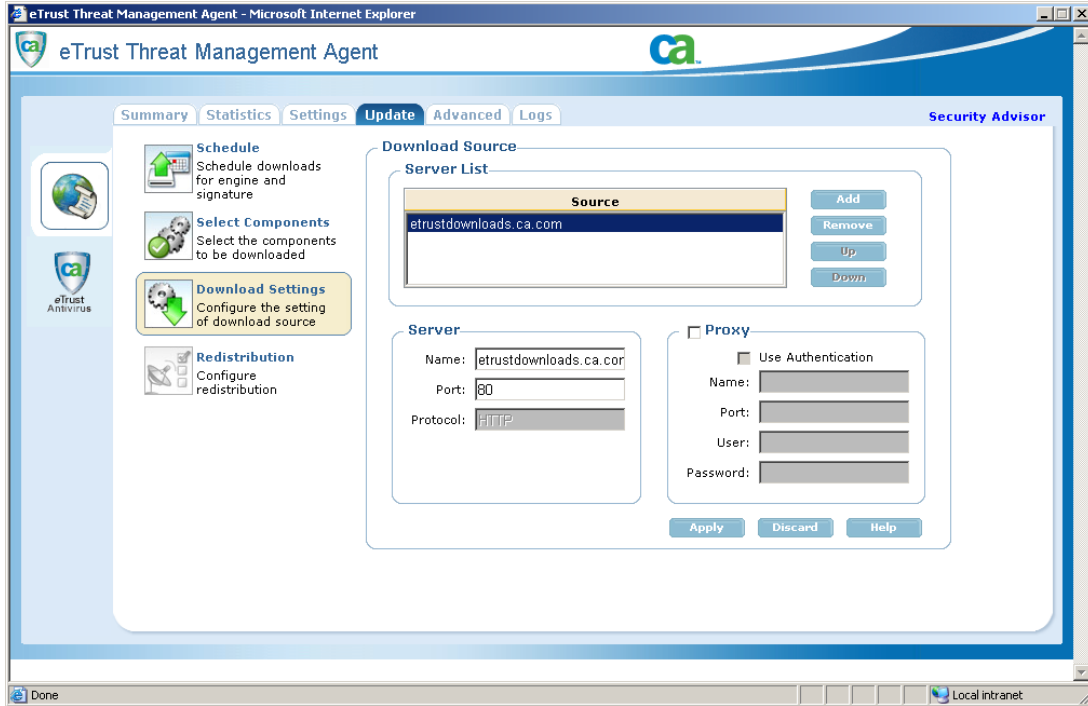
54. Select the "**Update**" tab. Set up daily updates to be done at a time when system traffic is expected to be low. Avaya recommends that definition updates be done at least once a week but no more often than once per day.



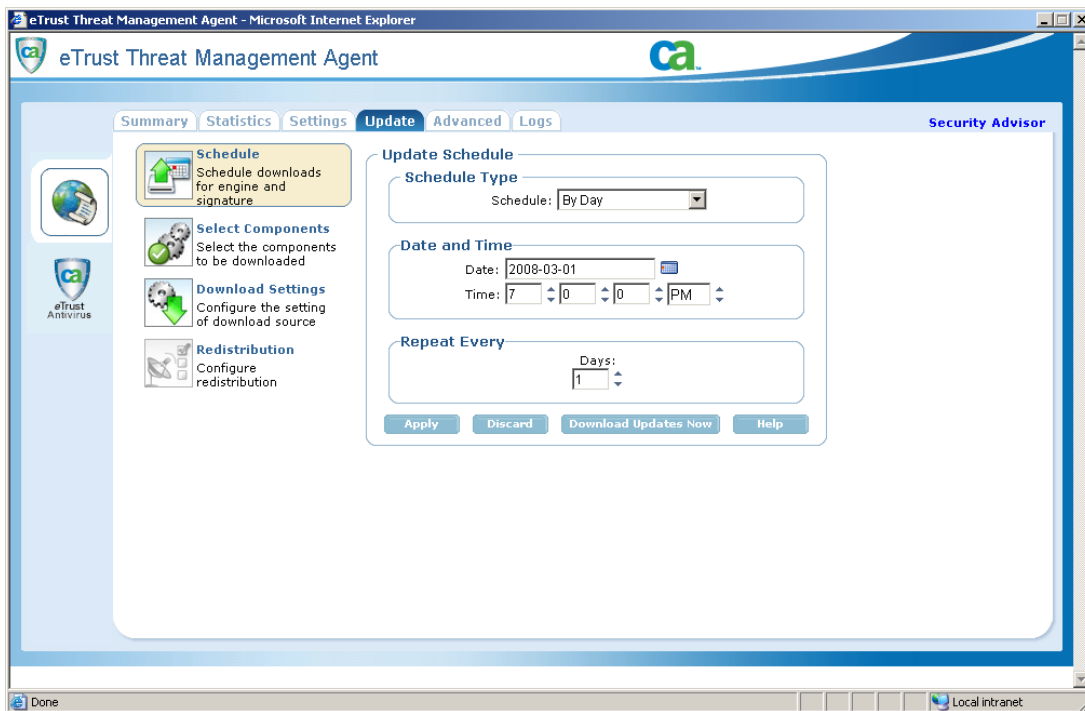
55. Click **Apply**. Click "**Select Components**" to be updated:



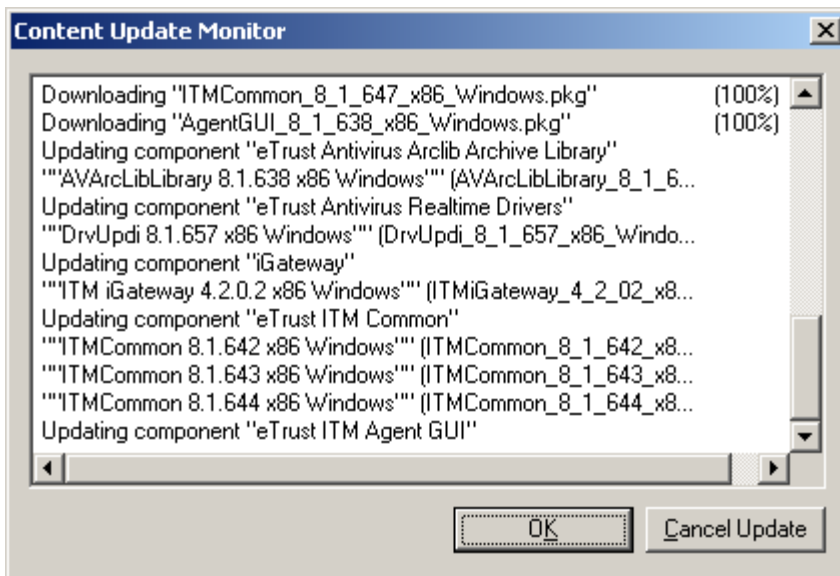
56. Click "**Download Settings**" By default, updates are downloaded from the CA server. If you wish, you can configure a local server instead (or in addition). Other update techniques are acceptable. The important points are a) signatures must be regularly updated, and b) updates must only happen when CallPilot traffic is expected to be low.

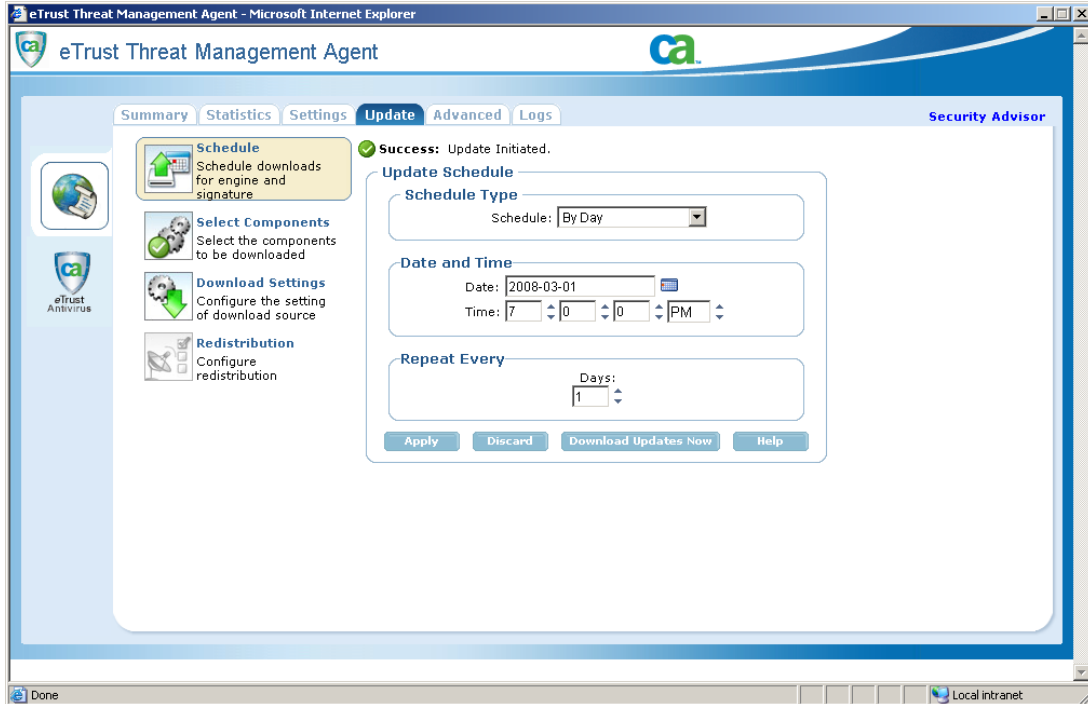


57. Go back to the **"Schedule"** screen

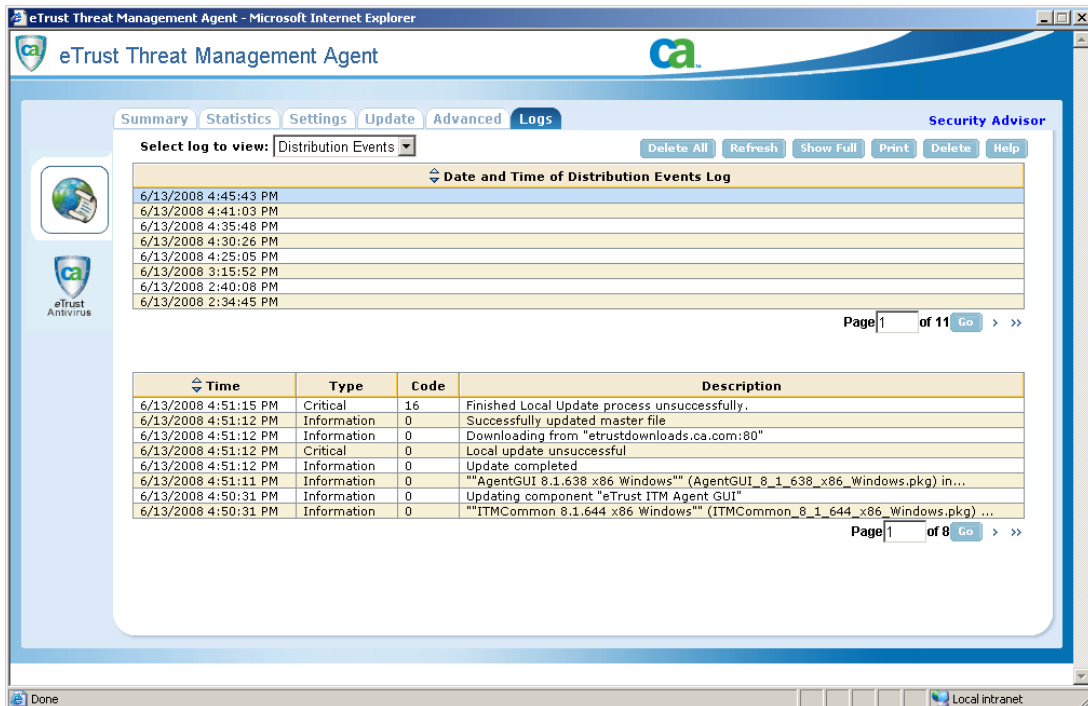


58. Click **"Download Updates Now"**. Ensure the download source is accessible and the update succeeds. The CallPilot server network settings must have proper DNS server(s) configured so the download server can be found. During updates, a new tray icon appears indicating update in progress. You can right click it to "Show update status"

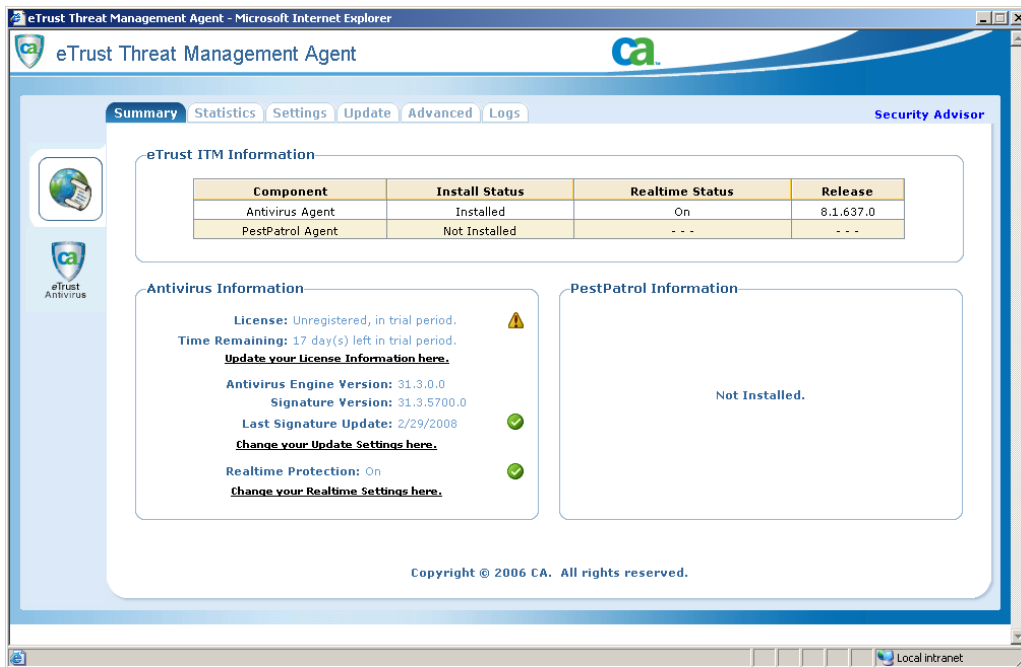




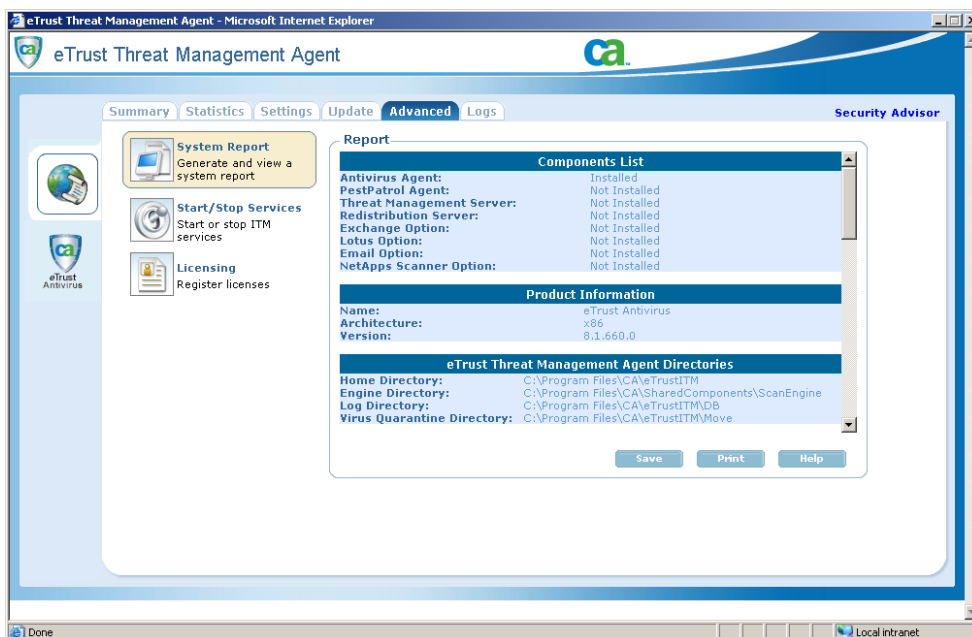
59. Select the “**Logs**” tab. In the drop-down box, select “**Distribution Events**”. Check that the update succeeded



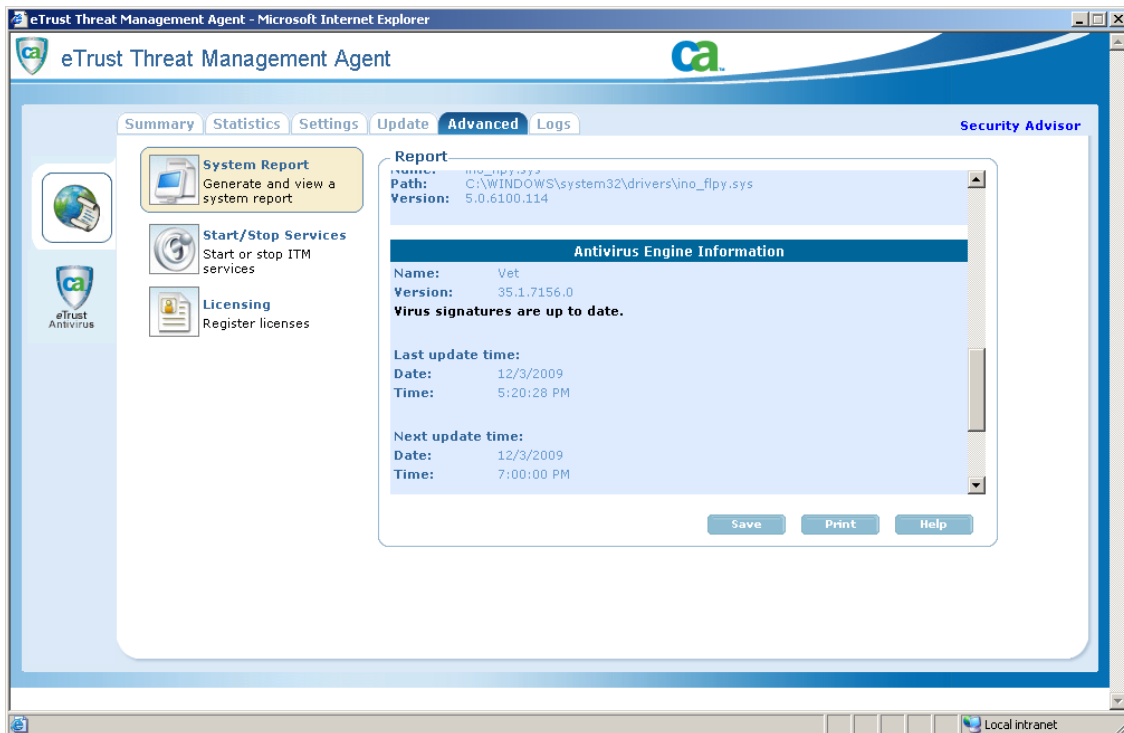
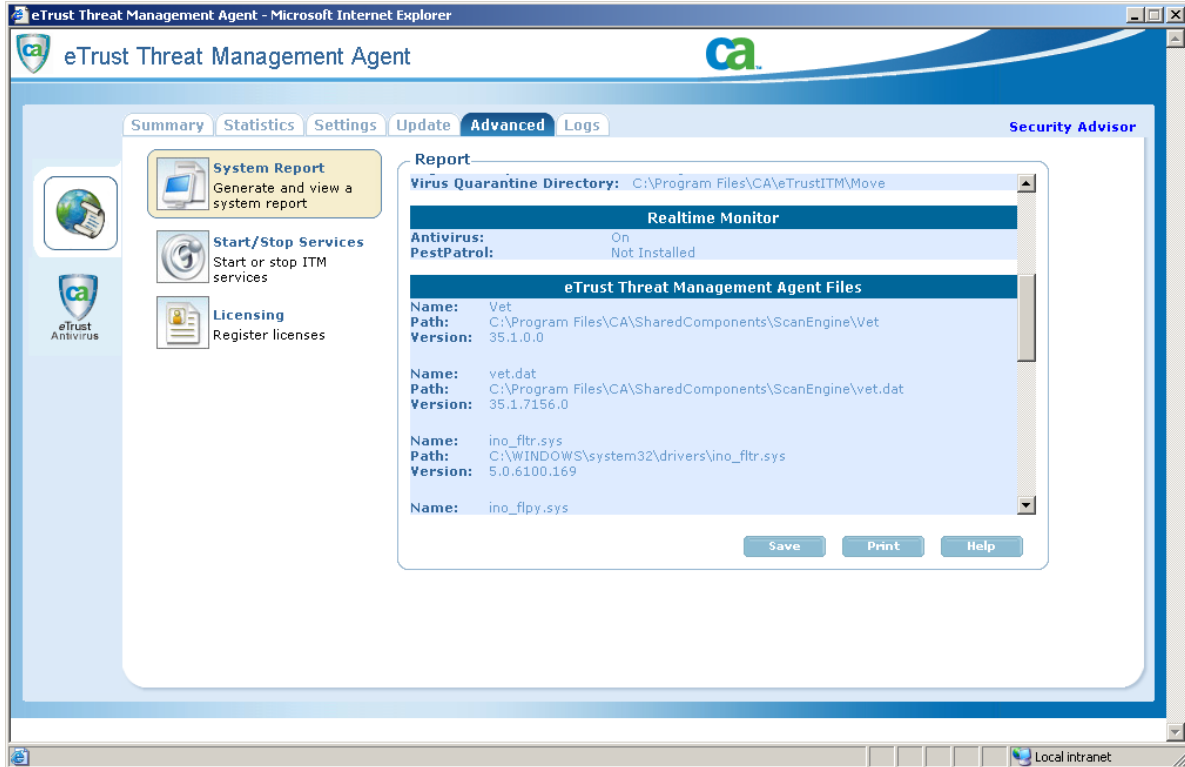
60. Select the “**Summary**” tab. Check the signature version to ensure that the virus definitions (signatures) got updated. (After a manual update, it may still say “No update performed”).)



61. To check the installation, you can select the “Advanced” tab and view the “System Report”. Compare it to the following screen shots.



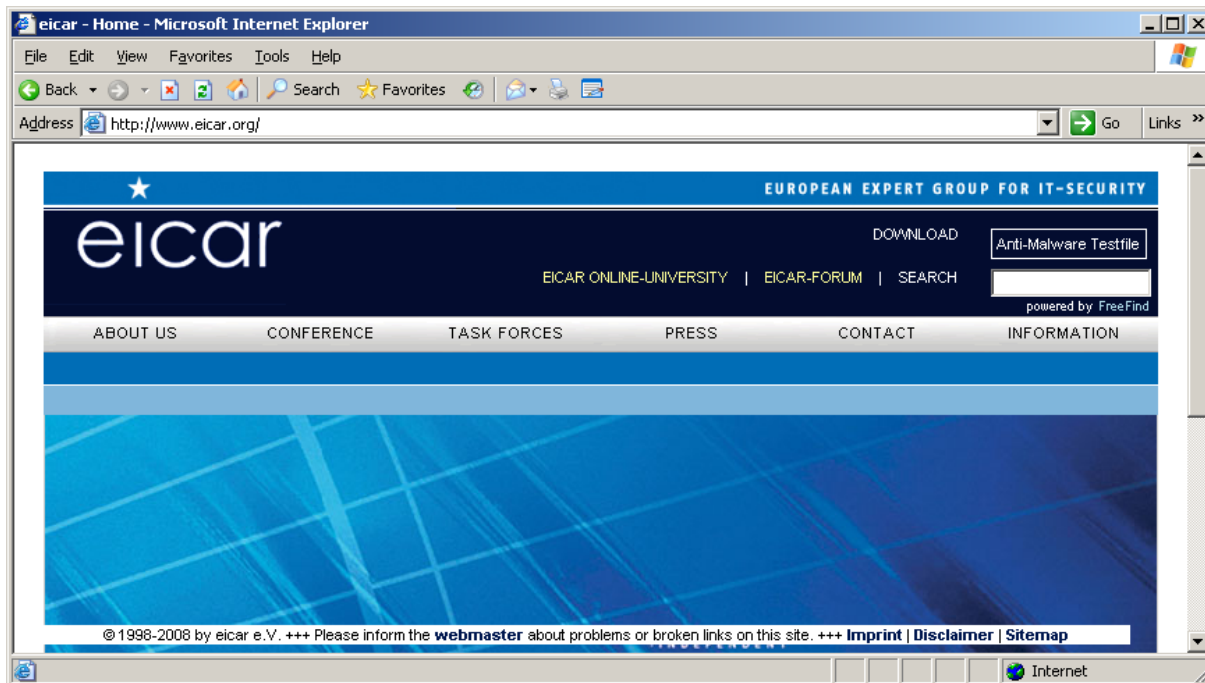
Scrolling down...



62. Close "eTrust Threat Management Agent" window.

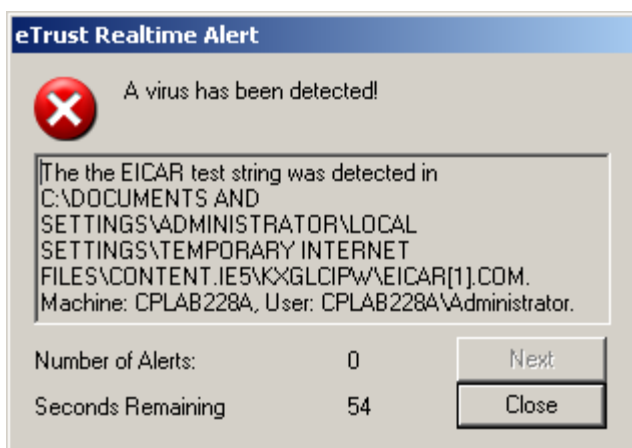
Testing CA Antivirus with the EICAR test virus

Open Internet Explorer and go to <http://www.eicar.org>



Select "**Anti-Malware Testfile**"

Try downloading "eicar.com", "eicar.com.txt", "eicar.com.zip", "eicarcom2.zip". You can also test the SSL enabled downloads. The AV software should block them all. (You may have to add the eicar site to the trusted sites list to carry out this test.)



Note: be sure to delete all instances of the eicar test files from the CallPilot server and empty the recycle bin. Otherwise they may result in ongoing virus alerts.

CA AntiVirus 8.1 Resource Usage

Services Started

When properly installed, three (3) additional services will be visible in the Windows Services applet:

- eTrust Antivirus Realtime Service
- eTrust ITM Job Service
- eTrust ITM RPC Service

Disk Space usage:

C drive: 43 MB

D drive: 85 MB

Process	Description	Typical Virtual Memory usage during normal CallPilot operation	Maximum Virtual Memory usage observed
Authtool.exe			
Compver.exe	Update and Patch Distribution		
ConfigTool.exe			
Eavdisk.exe			
eITMURL.exe			
EnableWinICF.exe			
iGateway.exe	iTechnology Application Server	13.8 MB	21 MB
InoCmd32.exe			
InoDist.exe			
InoRpc.exe	ITM RPC Service (listens for administrative server's discovery and policy requests)	200 KB	5 MB
InoRT.exe	Antivirus Realtime Service (provides real-time, on-access scanning)	21 MB	50 MB
InoTask.exe	ITM Job service (schedules background tasks such as scan jobs and content update downloads). Runs scheduled scan.	24 MB	52 MB (during scan)
ITMDist.exe			
Phonhome.exe			
Realmon.exe		1.5 MB	5.4 MB
Shellscn.exe	eTrust Antivirus Shell Scanner		
SigCheck.exe			
Spar.exe	SPindle Archive		
Spintool.exe	Spindle Tool		
Transtool.exe	Translation Tool		
UnITMEng.exe			

Appendix-B

McAfee VirusScan Enterprise 8.5i NOT Authorized for use on CallPilot Servers

At the request of several customers who had experienced problems using McAfee VirusScan 8.5i on CallPilot servers, Avaya carried out extensive testing in an attempt to arrive at a configuration for VirusScan 8.5 that could successfully be used on CallPilot servers. McAfee support was also engaged in this effort.

McAfee VirusScan 8.5i testing has shown repeatedly that the product can cause outages on CallPilot servers. In some cases the outages are not automatically recovered and system problems are created that may not be noticed until CallPilot traffic increases during a later busy period. A manual system reboot was often required to restore proper service. The problems were not restricted to any particular CallPilot platform or release.

The most serious design issue with McAfee VirusScan is that its “On-Access Scanner” process (McShield.exe) is set to run at “AboveNormal” execution priority, whereas CallPilot application processes run at “Normal” priority. Consequently, the on-access scanner will pre-empt CallPilot processes. If the on-access scanner only used very short bursts of CPU time, this would not be a problem. However, when the on-access scanner needs to scan a large file (in particular, a large compressed file), the scan can take a long time (many seconds, possibly minutes). During this time, CallPilot processes are starved of CPU time. This can result in timeouts of critical protocols needed by CallPilot and sometimes results in CallPilot ending up in an impaired state from which it does not fully recover automatically.

This problem is compounded by the fact that VirusScan performs its on-access scan even on its own virus definition package as it is downloaded during a definition update process. This package consists of multiple large files, some of which are compressed. Therefore, even if a customer never intentionally copies large files onto their CallPilot server, the regular definition update process will still result in lengthy on-access scanning that could result in a CallPilot service outage. This can happen even when virus definition updates are scheduled to occur at off-hours.

Avaya attempted to address this problem by trying to set up scanning exclusions so the definition files would not be scanned. This did help, but, still outages did occur when McAfee included unexpected files in its update package. In spite of repeated requests, McAfee failed to provide any configuration instructions to definitively solve this problem.

Since an antivirus product cannot properly protect a CallPilot server without both on-access scanning and regular definition updates, the McAfee VirusScan 8.5 product is not suitable for use on CallPilot servers and Avaya does not authorize it.

Testing was carried out on McAfee VirusScan 8.5i with Patch 4 and with Patch 5. McAfee did acknowledge a problem with high CPU use during definition updates, and these patches did include a fix that reduced the length of the CPU spike. However, the patches did not solve the

problem sufficiently to eliminate the chance of a CallPilot outage. Our trial customer still experienced multiple outages following definition updates, even with all available patches and all exclusions in place. The problems only went away when definition updates were completely disabled – this is not an acceptable workaround.

In addition to high CPU usage, McAfee VirusScan has high memory usage. On some CallPilot platforms, this high memory usage can easily cause problems, particularly when a customer is using the ePO (ePolicy Orchestrator) management feature. Also, the “Access Protection” feature of VirusScan needs to be carefully configured so that it does not break CallPilot features in subtle ways.

Avaya has submitted product improvement recommendations to McAfee and will consider testing future releases of McAfee antivirus products if those products are improved. Other vendors have been able to produce effective AV products without the issues Avaya encountered on McAfee VirusScan. CallPilot customers should install one of the authorized antivirus solutions.

Appendix-C

This appendix provides Installation and Configuration procedures for CallPilot 4.0 and 5.0 servers utilizing the **McAfee VirusScan Enterprise 8.7i** anti-virus application.

IMPORTANT NOTE - PLEASE READ!

Avaya tests antivirus products only to ensure that CallPilot operates properly when the AV product is installed and configured according to these instructions. Avaya does not test the effectiveness of the AV product at detecting viruses. All AV products require regular definition updates in order to protect properly. It is the responsibility of the customer, possibly working with the AV vendor, to ensure that virus definitions are kept up to date. For more information, read this document.

Description

This document provides installation and configuration guidelines for McAfee VirusScan Enterprise 8.7i on a CallPilot server and also covers the use of McAfee ePO. This document should not be considered a replacement for the McAfee VirusScan and ePO product documentation. The intention is to show how to install and configure VirusScan in a way that minimizes the impact to the proper operation of a CallPilot server while still providing a high degree of protection from malware. This document does not apply to CallPilot standalone web server machines – that is up to the customer (but this document might still be useful).

Tested: McAfee VirusScan Enterprise 8.7i with Patch 1 trial downloaded Sept 29/2009 and McAfee VirusScan Enterprise 8.7i with Patch 2 trial downloaded Nov 5/2009.

These guidelines cover four main topics:

- Product features description;
- Step by step installation instructions;
- Step by step configuration instructions.
- Information on the use of ePO

All necessary documentation concerning the McAfee VirusScan Enterprise software can be found on the VirusScan product CD and can be downloaded by customers from the McAfee download site:

Product Features

- McAfee VirusScan® Enterprise 8.7i incorporates best-of-breed McAfee anti-virus, and rootkit protection for advanced end-point protection. Only the English version is supported on CallPilot servers since CallPilot runs the English version of Windows.
- McAfee VirusScan 8.7i from McAfee is a combined desktop and server solution combining VirusScan and NetShield products. (Note: McAfee was previously known as Network Associates)
- VirusScan 8.7i features memory scanning to detect memory resident viruses. It can detect viruses within compressed files. It is able to use heuristic scanning to find viruses that are not included in definition files.

- Antivirus scans and definition updates work properly even when the local console is in a logged-out state.
- A powerful “Access Protection” feature provides configurable settings to protect against many specific malware behaviors. The “AccessProtectionLog” file shows what behaviors were blocked or reported.
- There is an ability to detect “unwanted” programs. You can select categories of programs from the categories included in the current DAT file, exclude specific categories or files, or add your own programs to detect with using the Unwanted Programs Policy feature.
- McAfee VirusScan Enterprise has an Alert Manager (Local Alerting). This feature allows you to generate SNMP traps and local event log entries without installing Alert Manager Server locally.
- VirusScan has an ability to scan Java Script and VBScript scripts before they are executed on the CallPilot server, however use of this feature is not recommended on CallPilot since it leads to a large increase in memory consumption. Since the browser on CallPilot should be used only rarely, CallPilot is not at great risk from this type of malware.

For more detailed information about product features consult the VirusScan documentation and on-line help or contact McAfee. VirusScan is not an Avaya product. It is not sold or supported by Avaya. Avaya does not evaluate the virus detection performance of AV products.

Product Deficiencies

- The Virus Definition update process is very resource intensive and may impact CallPilot performance. It should be performed only when the system is expected to be idle. Sometimes definition updates require system reboots.
- On-access scanning is done by high-priority process McShield.exe. This potentially starves CallPilot of CPU, resulting in timeouts and impact to user operations when large compressed files (e.g. PEPs) are copied onto the system when it is under load.
 - o Note: A workaround is documented below for this issue. Disable on-access scanning temporarily to avoid this when required.
- If a virus scan finds a virus on the CallPilot server, there is no built-in way to alert a remote administrator. The administrator must manually check the CallPilot server for virus indications in the log file. McAfee has a separate component called the “Alert Manager” which can be configured to receive virus alerts from CallPilot and other servers. Unless the customer will be regularly checking the CallPilot server console, Alert Manager should be installed to ensure that virus detections are noticed. The instructions given here do not cover the installation and configuration of the Alert Manager. Consult the VirusScan documentation and on-line help.
- System reboot may be required after installation. Therefore a maintenance window needs to be scheduled if the system is in production

ePolicy Orchestrator (ePO)

For more information on ePO, see the ePolicy Orchestrator section later in this document.

- McAfee’s ePolicy Orchestrator (releases 3.6.1, 4.0 or 4.5) provides a way to centrally manage the anti-virus configuration and definitions of many computers running VirusScan. The server, console, database and remote console components of ePO must never be installed on a CallPilot server. However, under certain conditions, it is acceptable to install

the ePO agent on a CallPilot server to allow its anti-virus configuration to be centrally managed. Consult McAfee documentation for ePO.

- The following conditions should be observed when installing the ePO agent on CallPilot servers:
 - o If the ePO agent is installed on a CallPilot server, you should take care that AV scans, definition updates, and management activities occur only at times of very light CallPilot system load.
 - o The anti-virus configuration policy installed via ePO should match that described in this document as much as possible. Since the policy needed for CallPilot servers will likely differ from that needed for normal desktop PCs, CallPilot servers need to be managed as a separate group. You should create a new named policy within ePO specifically for CallPilot servers.
 - o Be sure that the required policies are being properly applied by ePO to the CallPilot server. Ensure that other policies are not being inherited within the ePO directory in a way that overrides the required CallPilot policies. Check the policies by observing them on the CallPilot server by running the VirusScan console. If the VirusScan policies on the CallPilot server do not match those described in this document, make changes to the ePO policy so that the correct policies are seen to be in effect on the CallPilot server.
 - Never put the CallPilot server into service with incorrect VirusScan policies since the CallPilot might stop working properly.
 - o **Virus definitions must only be pushed to a CallPilot server at times CallPilot is expected to be idle.**
 - o The ePO agent software should be installed on the D drive on CP4 systems, if possible. Please ensure that the CallPilot system drive (where the OS is installed, usually C) still has at least 135 MB free after installing the AV software. (Note: files on the desktop of any Windows userid also consume space on the system drive).
 - o The VirusScan On-Access Scan should not be set to scan when reading files, particularly when My CallPilot is being hosted on the CallPilot server. Set it to scan only when writing to disk.
 - o Do not install VirusScan by remotely pushing it via ePO onto a CallPilot server.
 - o Be very careful using global updating. Be sure that CallPilot servers are only updated at times of very low CallPilot call traffic.
 - o A CallPilot server must never be configured as a “SuperAgent”.
 - o The “Agent to Server Communication Interval” should not be set to less than one hour.
 - o Note: Avaya recommends that on-demand scan CPU utilization be set to 70%, CPU Utilization for a Virus scan should never be set to 100%. CallPilot call handling will be impacted.

Installation and Configuration Instructions

Use a fully patched and Anti-Virus protected PC to download the latest AV software and virus definitions and burn the files onto a CD so that it can be brought to the CallPilot server without using the network. (It is dangerous to use the Internet to download the initial virus definitions after a fresh install of Anti-Virus software. An unprotected computer can become infected in the time it takes to download updates.)

For McAfee VirusScan, definitions and updates can be downloaded from (Note, URL is subject to change):

http://www.mcafee.com/apps/downloads/security_updates/superdat.asp?region=us&segment=enterprise

McAfee uses the word “DAT” for virus definition files. You will also need the latest “Engine”. Download a “SuperDAT” file to get the latest Engine and the latest definitions in a single download. The file is provided in a self-extracting executable. Typically, the SuperDAT file will be 120 MB or more. (A few years ago they were only a few MB.)

For best security, a CallPilot server must never be connected to the Internet unless it has the latest CallPilot OS Security PEPs, all OS hotfixes authorized for CallPilot and has Anti-Virus software installed with the latest virus definitions. Therefore, unless the network is very well-protected, disconnect the CallPilot Server from the network by unplugging both ELAN and CLAN until you have installed the Anti-Virus Software. Be sure you remember where the cables should be plugged back in.

Uninstall any existing Anti-Virus software. Problems will occur if more than one anti-virus product is installed at a time. Reboot if required.

Before installing Antivirus software - install all applicable CallPilot OS Security PEPs from CD. Install any additional, authorized hotfixes from CD.

If installed according to the instructions given here, antivirus software should have no noticeable impact on CallPilot performance and capacity for normal messaging-related operations. Certain exceptional operations that involve updating a large number of files may operate significantly slower on some platform types due to the added cost of virus scanning. Examples are: software upgrades, PEP installs, restore from backup. You may want to temporarily disable On-Access scanning monitoring while performing those operations.

Disk Space Requirements

When installed on C drive:

C drive: uses 371 MB (note: patch 1 version used more disk space)

When installed on D drive:

C drive: uses 209 MB

D drive: uses 179 MB

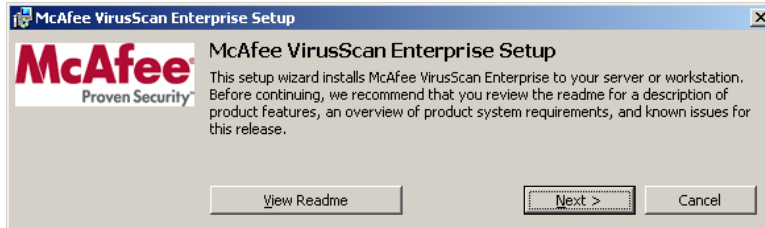
Memory commit charge: used: 92 MB (note: patch 1 version used more memory)

Tested: McAfee VirusScan Enterprise 8.7i with Patch 2 trial downloaded Nov 5/09

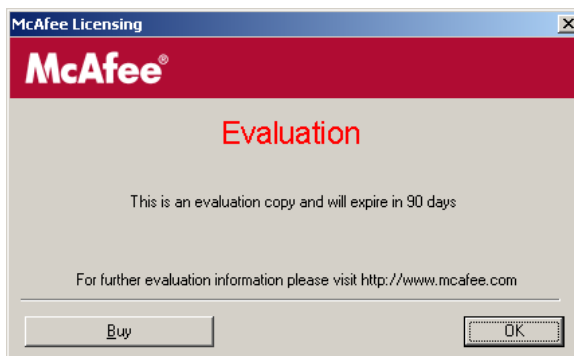
McAfee 8.7i Installation Step by Step Instructions

Installation and configuration of McAfee 8.7 can be expected to take about one (1) hour (more if a full anti-virus scan is run during the install).

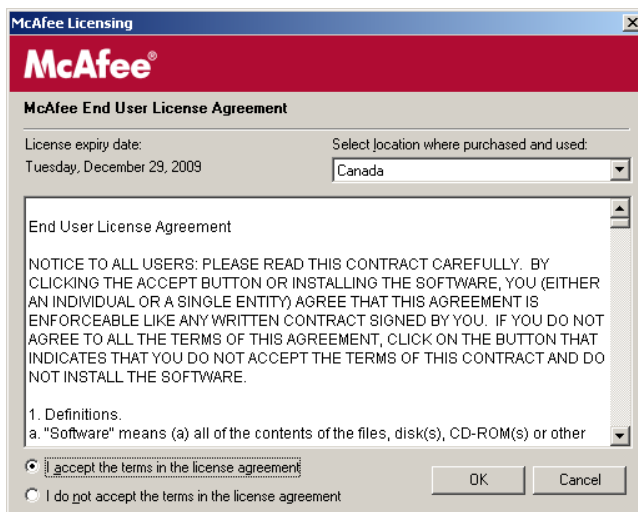
1. Double-click "**SetupVSE.exe**". (Note, the method for initiating setup may vary according to the exact McAfee product.)



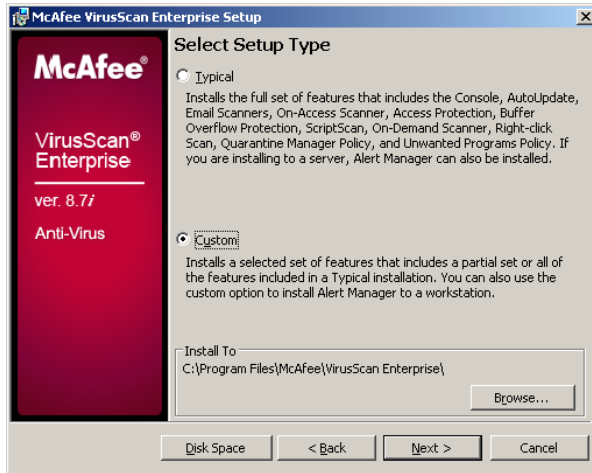
2. Click **Next**



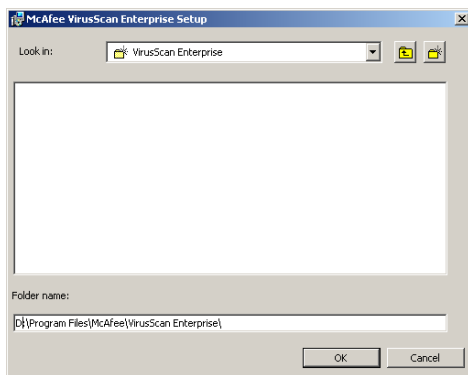
3. Click **OK**. (NOTE: Evaluation versions must not be used on production systems at customer sites. Use only a properly licensed version so that it will not expire).



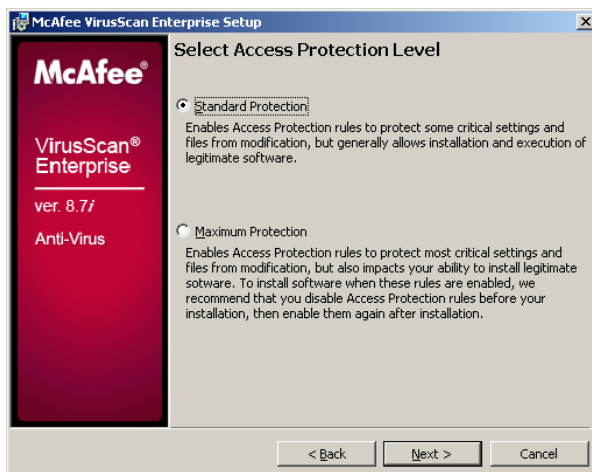
4. Select location where purchased and used. Read End User License Agreement. Select **"I accept..."**, Click **OK**



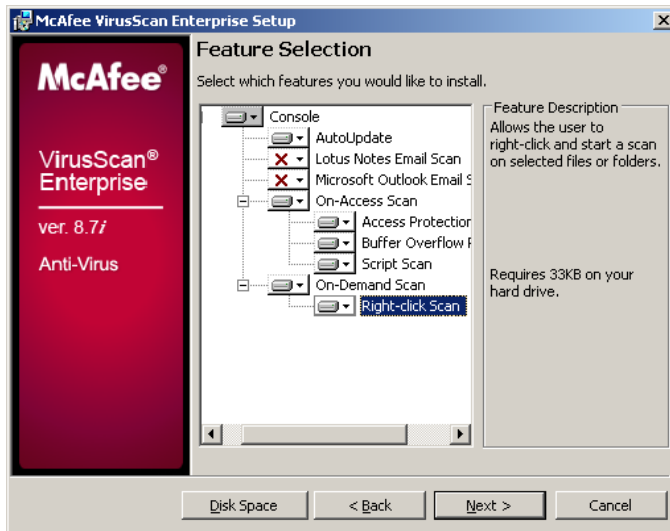
5. Select **"Custom"**. For CallPilot 4.0, click **Browse** and change the install folder so it begins with **D**. For CallPilot 5.0 and later, just use the default install folder on **C**.



6. Click **Next**



7. Click **Next**.



8. For "Lotus Notes Email Scan" and "Microsoft Outlook Email Scan" click and select "**This feature will not be available**". Click **Next**.



9. Do not select "Install Alert Manager Server". Click **Next**.



10. If your site has an AutoUpdate repository list file that you wish to import, you may optionally select "Import AutoUpdate repository list". Click **Next**.



11. Since CallPilot servers are accessed at the Windows login level only by trusted personnel, it is not usually necessary to protect the configuration with a password, or to hide the McAfee shortcuts. (If required, however, you may choose to do so.) Click **Next**.



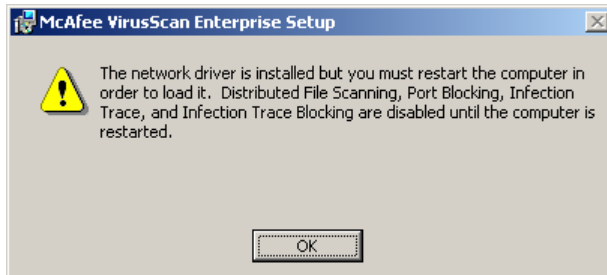
12. Click **Install**.



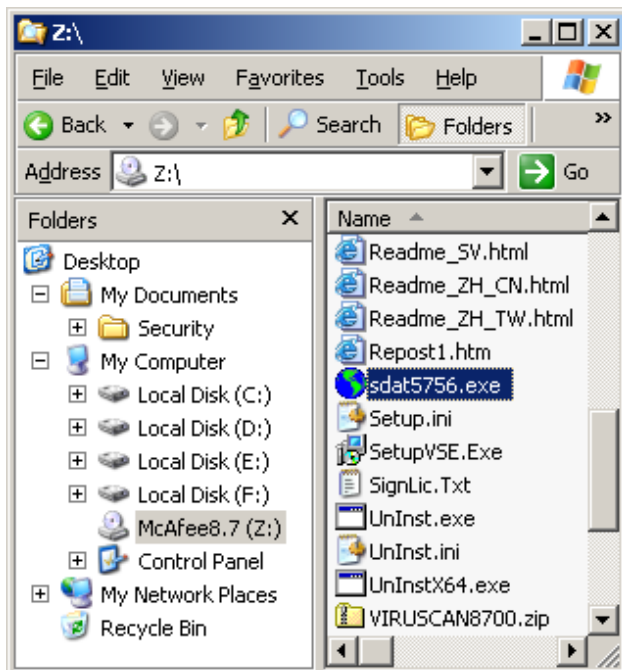
After a few minutes, you will see:



13. Uncheck the "Update Now" and "Run On-Demand Scan" check boxes. (Since the LAN is disconnected at this point, the update will not work. We will run an on-demand scan after we have manually updated the definitions.). Click **Finish**.



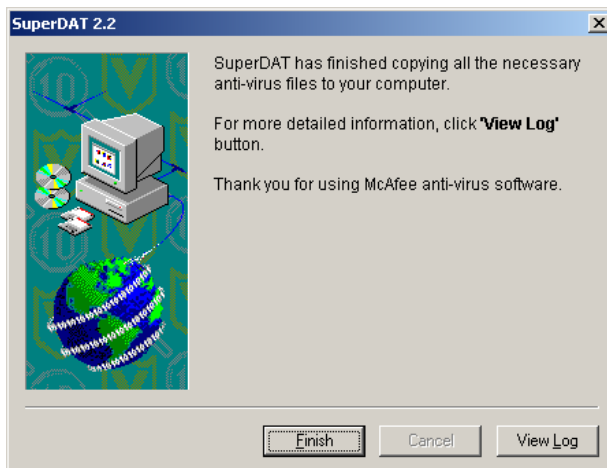
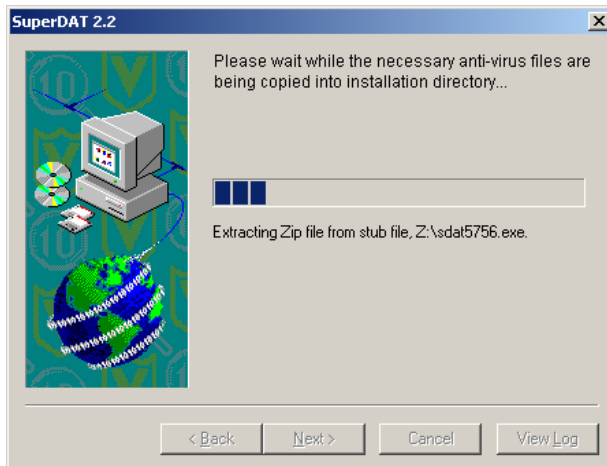
14. Click **OK**. VirusScan has now been installed. Note that two entries will appear in the Control Panel – Add/Remove Programs list: "McAfee Agent" and "McAfee VirusScan Enterprise" – both must be uninstalled to completely uninstall the McAfee software. A reboot is recommended at this point. (Note: sometimes some services may fail to start after the reboot. See section on "Issues" later in the document.)
15. After the reboot, you should install the latest available Patch for VirusScan 8.7. Contact your McAfee support representative to obtain this patch. You will need a "Grant Number" to get the patch. (Avaya testing used Patch 1 and Patch 2 only but the latest available patch should always be used by customers.)
16. Now, update the virus definitions and scan engine using the SuperDat file you previously burned to CD.



In Windows Explorer, double-click on the **sdatxxxx.exe** file.



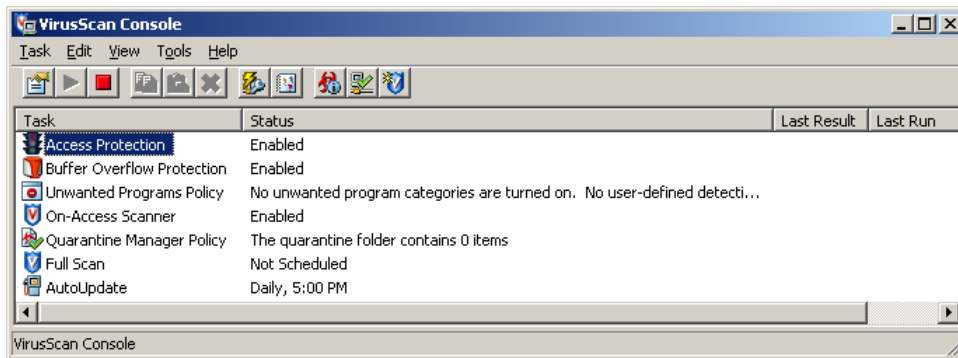
17. Click **Next**



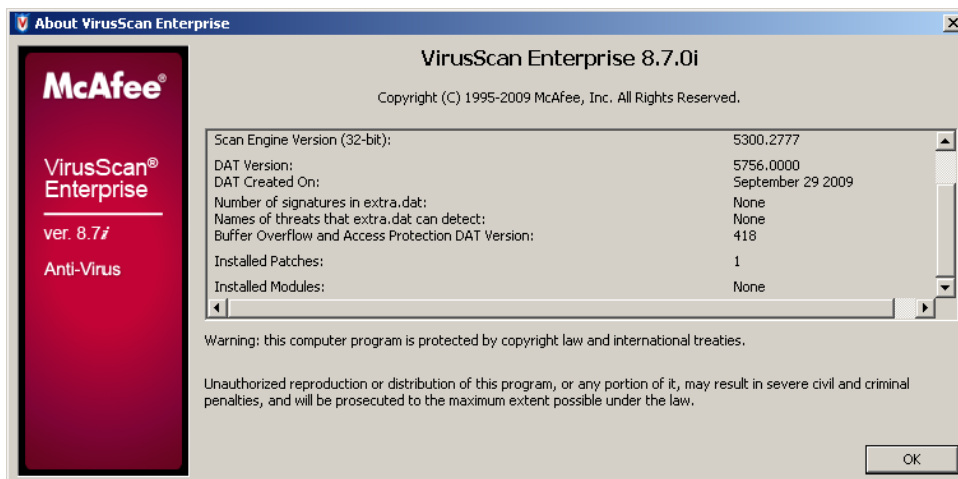
18. Click **Finish**. The CallPilot system may seem slow at this point and may require some time before performance improves.

Step by Step Configuration Instructions

1. Start - Programs - McAfee - VirusScan Console

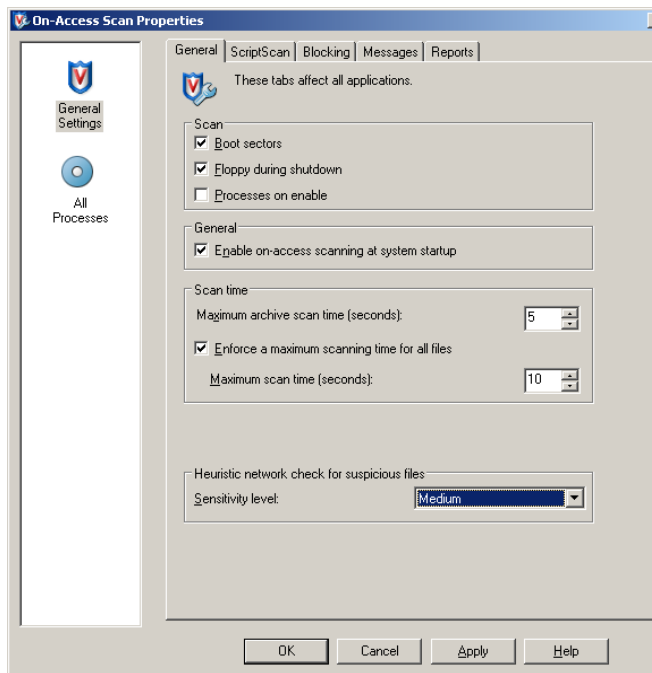


2. You can check the date of the virus definitions, scan engine version and installed patches by using the Help menu. Select "About VirusScan Enterprise".

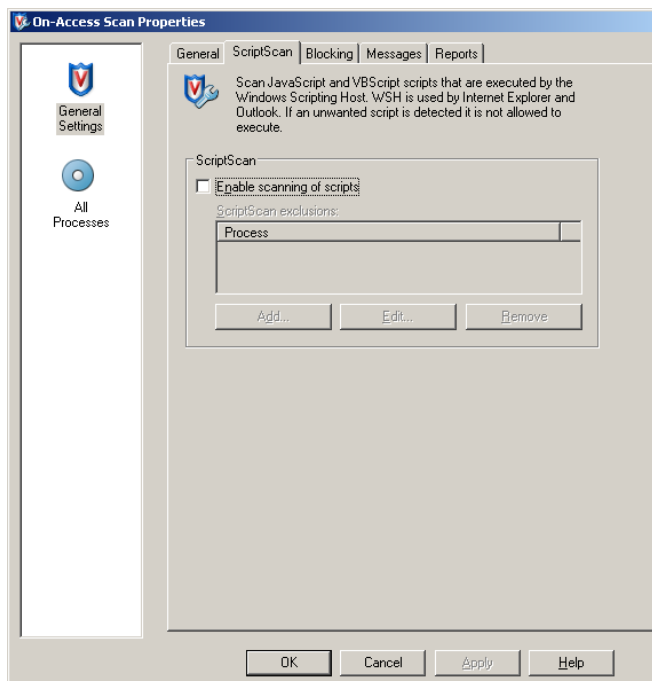


3. Click **OK**.

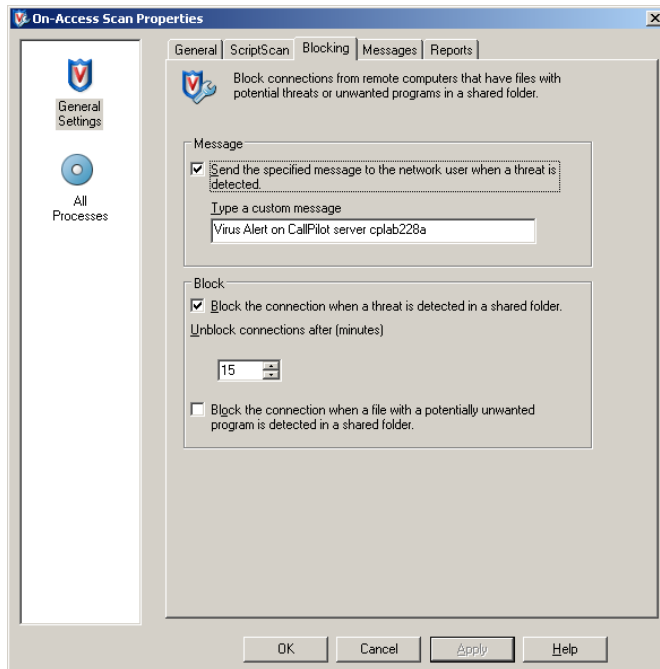
4. In the VirusScan Console, double-click "**On-Access Scanner**"



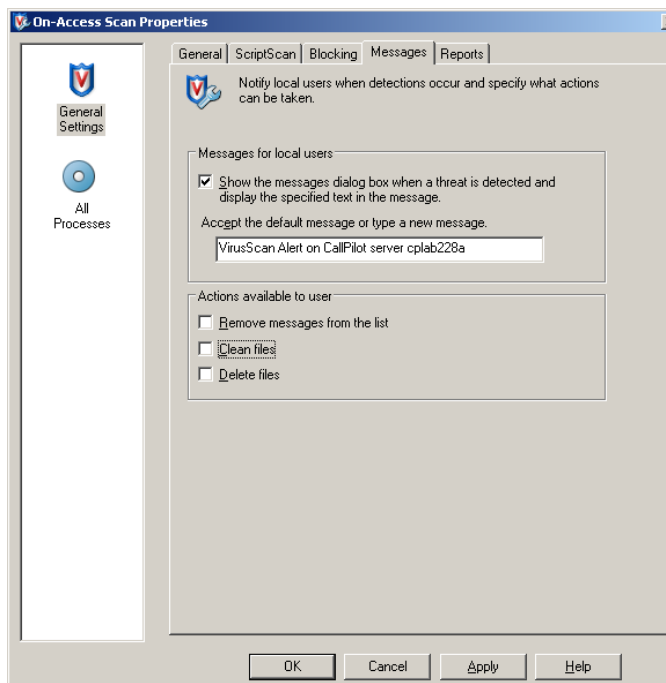
5. With "General Settings" selected on the left, change the Scan time "Maximum archive scan time (seconds)" to **5 seconds**. Change the "Maximum scan time (seconds)" to **10 seconds**. Change the "Heuristic network check for suspicious files" sensitivity level to "**Medium**". Click **Apply**.



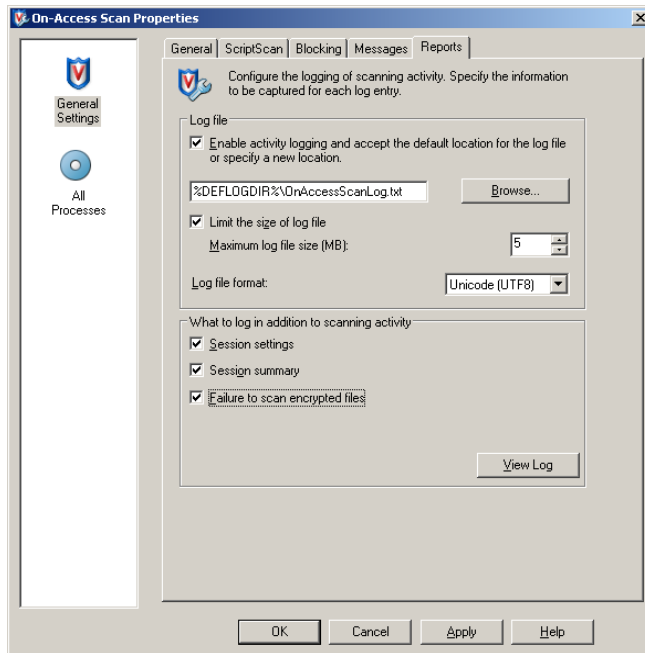
6. Select the "ScriptScan" tab. Ensure that "**Enable scanning of scripts**" is **not** checked. This feature can greatly increase memory usage, resulting in system problems.



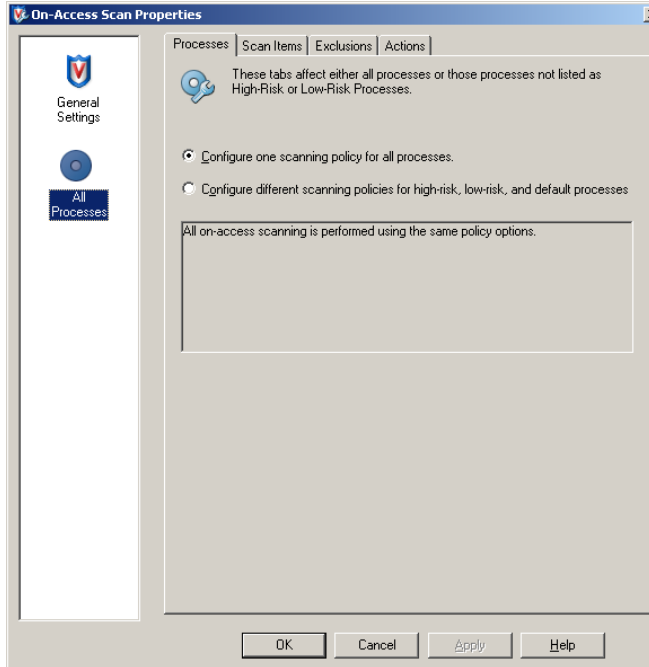
7. Blocking tab. Under "Message", check "**Send the specified message ...**" and type an appropriate message to send. It is a good idea to include the computer name of the CallPilot server in case the site has more than one CallPilot. Under "Block", for "Unblock connections after", set to **15 minutes**.



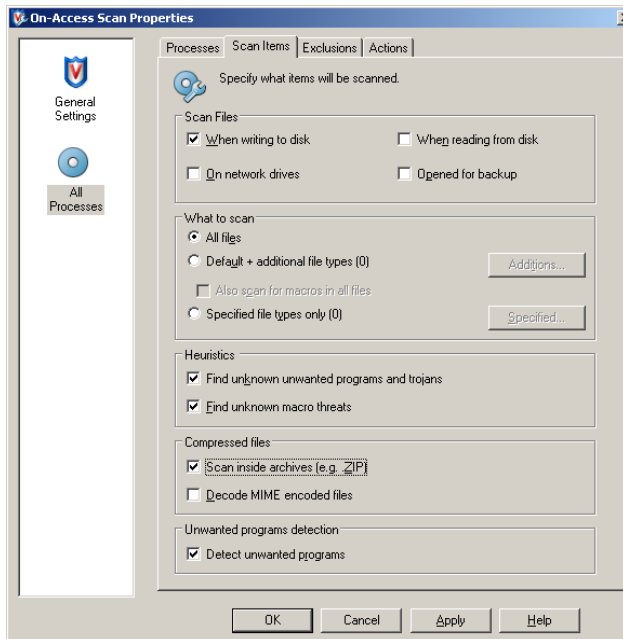
8. Messages tab. Fill in the computer name into the message box. Uncheck "**Remove messages from the list**" and "**Clean files**".



9. Reports tab. Set the maximum log file size to **5 MB**. Check "**Session settings**" so that setting changes are logged. Check "**Failure to scan encrypted files**". Click **Apply** to save all the On-access scanning settings.
10. Click "**All Processes**" at the left.

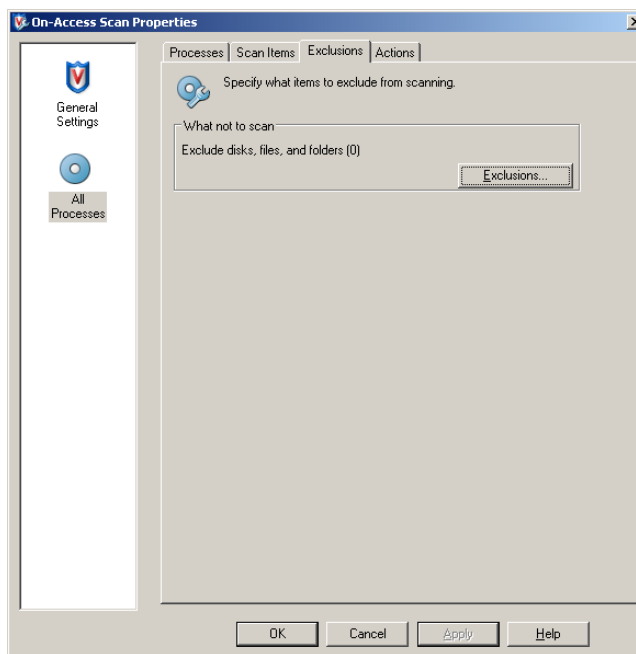


11. Select the "Scan Items" tab.

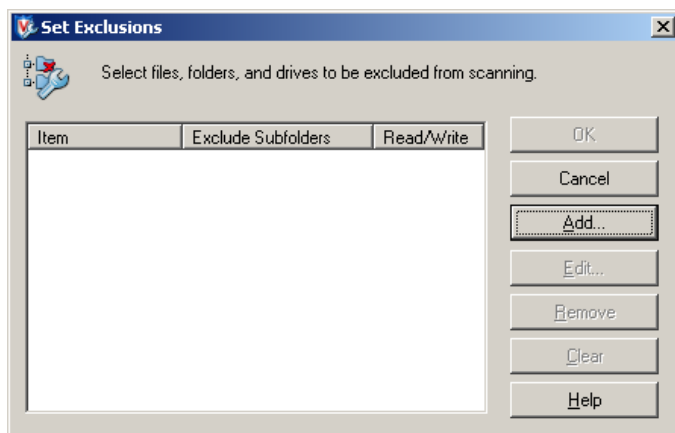


12. Uncheck "When reading from disk". Uncheck "Opened for backup". Check "Scan inside archives". Click **Apply**.

13. Select the "Exclusions" tab.



14. Click "**Exclusions...**".



15. Click **Add**.

Add Exclusion Item

What to exclude

☒ By name/location (can include wildcards * or ?):

[Browse...](#)

☒ Also exclude subfolders

☐ By file type (can include wildcards * or ?):

[Select...](#)

☐ By file age:

Access type: Minimum age in days:

Modified 1

☐ Files protected by Windows File Protection

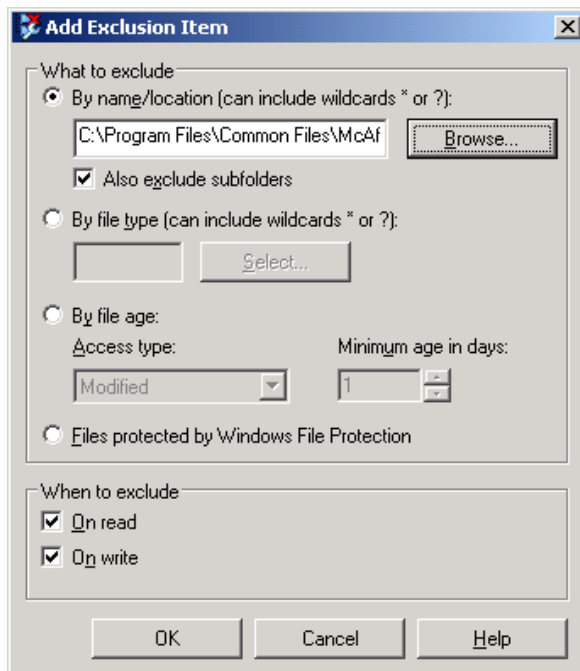
When to exclude

☒ On read

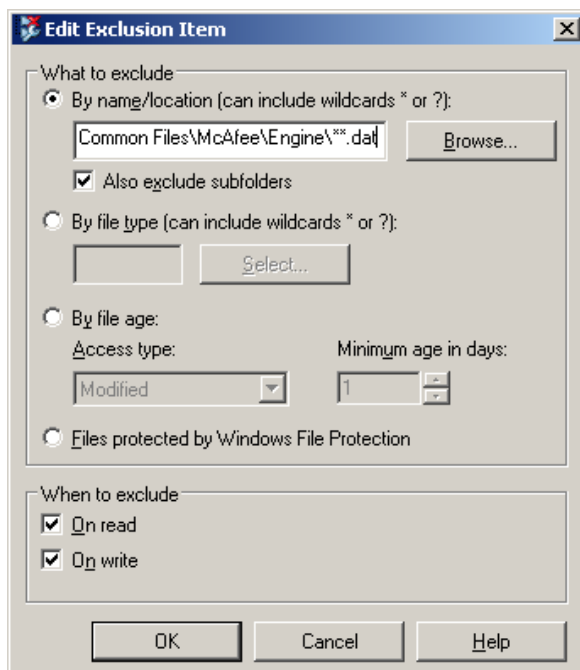
☒ On write

[OK](#) [Cancel](#) [Help](#)

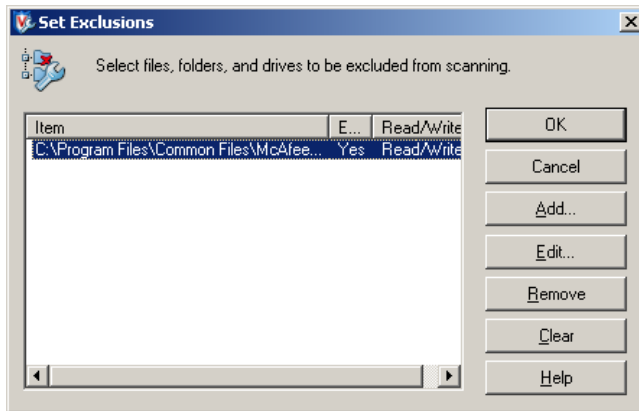
16. Select "Also exclude subfolders", then click **Browse** and browse to C:\Program Files\Common Files\McAfee\Engine and click **OK**. (Note: rather than browsing, you can also simply carefully type the path into the name/location box.)



17. Then click in the name/location field, scroll to the right and append "***.dat" to the string. (The double asterisk means "zero or more of any characters including back slash". It allows multiple depth exclusions.)

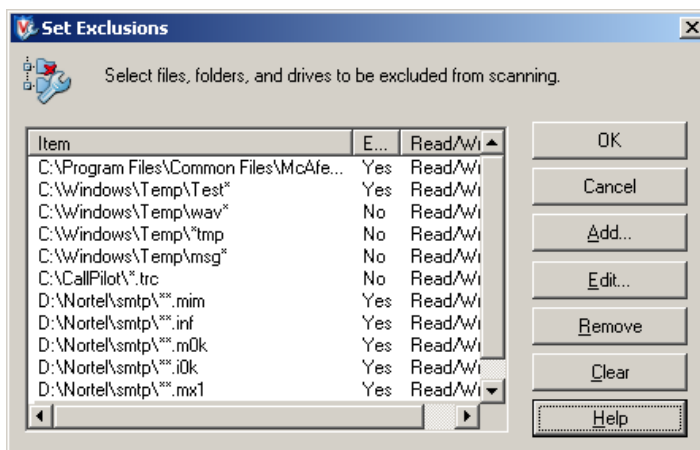


18. Click **OK**.

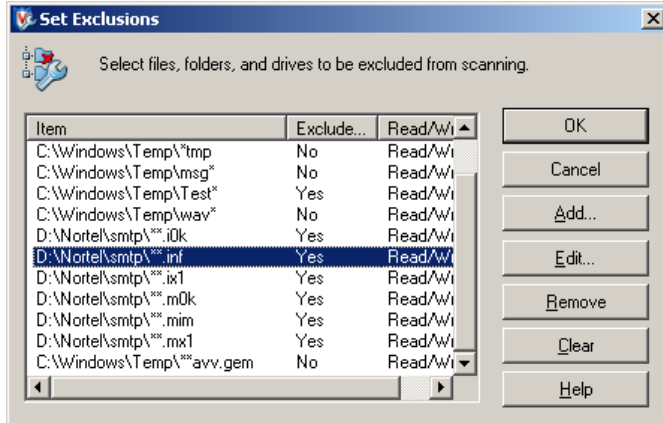


19. Add the following exclusions in the same way:

C:\Windows\Temp\Test*	(exclude subfolders)
C:\Windows\Temp\wav*	
C:\Windows\Temp*tmp	
C:\Windows\Temp\msg*	
C:\CallPilot*.trc	
D:\Nortel\smtp*.mim	(exclude subfolders)
D:\Nortel\smtp*.inf	(exclude subfolders)
D:\Nortel\smtp*.m0k	(that's letter m, number zero, letter k) (exclude subfolders)
D:\Nortel\smtp*.i0k	(that's letter i, number zero, letter k) (exclude subfolders)
D:\Nortel\smtp*.mx1	(exclude subfolders)
D:\Nortel\smtp*.ix1	(exclude subfolders)
C:\Windows\Temp*.avv.gem	

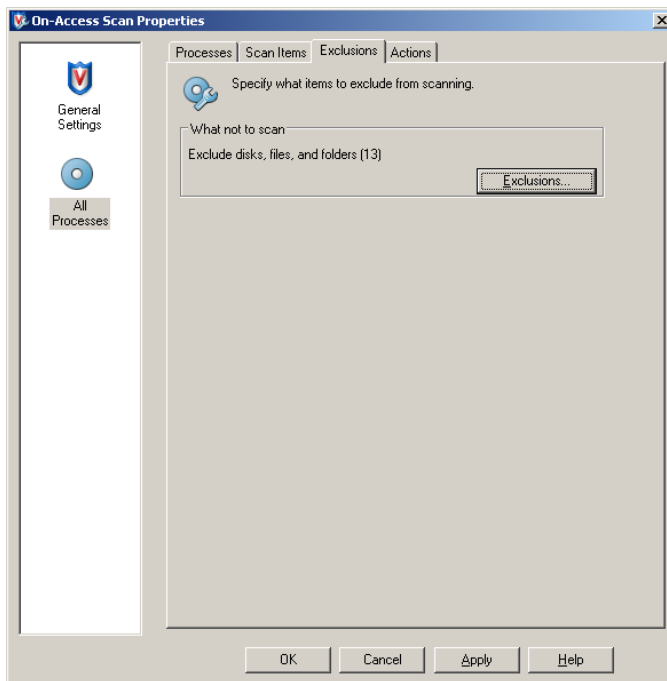


scrolling down

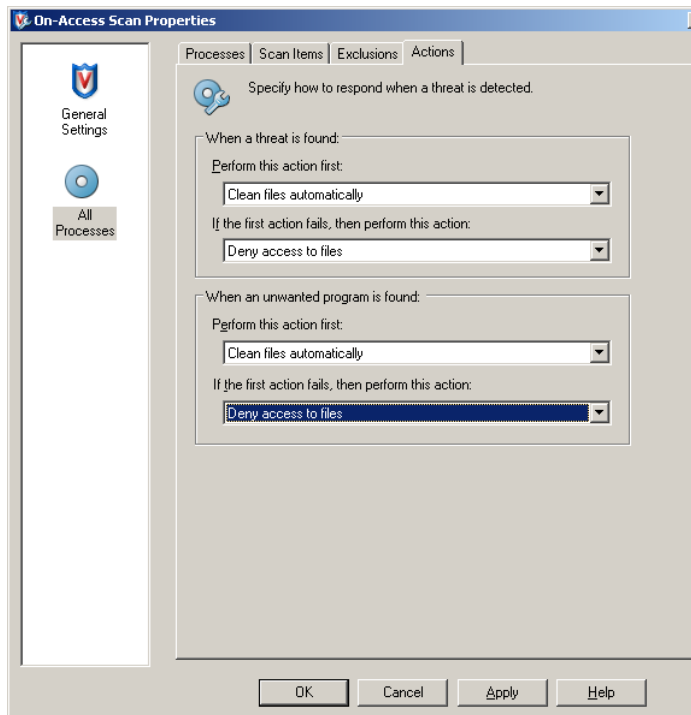


NOTE: On CallPilot High Availability systems, exclude the additional folder:
D:\Program Files\EMC AutoStart\<Domain Name>_<Computer Name>.
 (Where Domain Name is the name associated with the HA pair and Computer Name is the name of the specific node within that pair.)

20. Click **OK**.

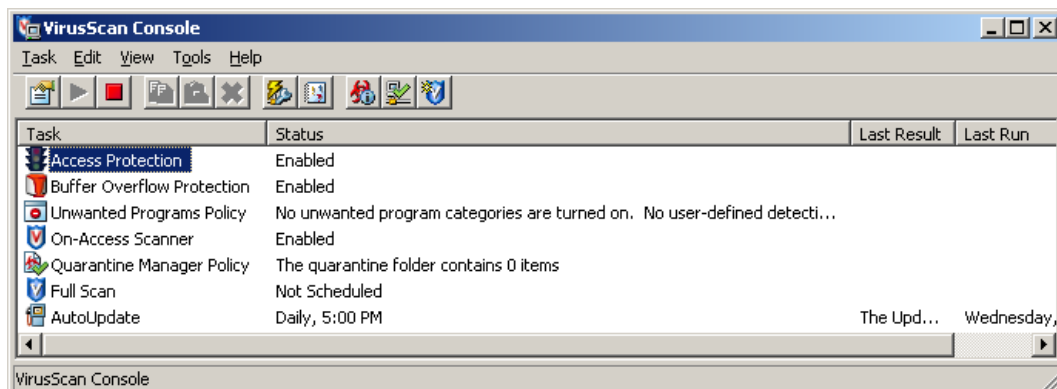


21. Select the "Actions" tab.

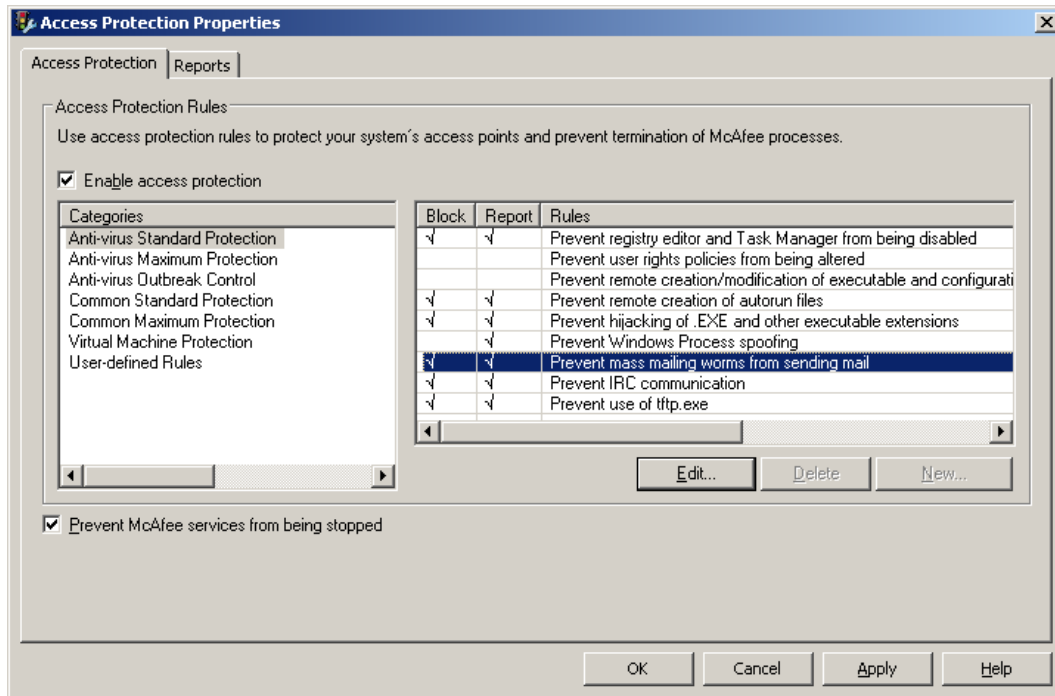


22. Under "When a threat is found", under "If the first action fails..." set action to **"Deny access to files"**. Under "When an unwanted program is found", under "If the first action fails...", set the action to **"Deny access to files"**. (In case the AV software has a "false positive" and flags a legitimate file as a virus, we wish to be able to restore the file.) Click **Apply**.

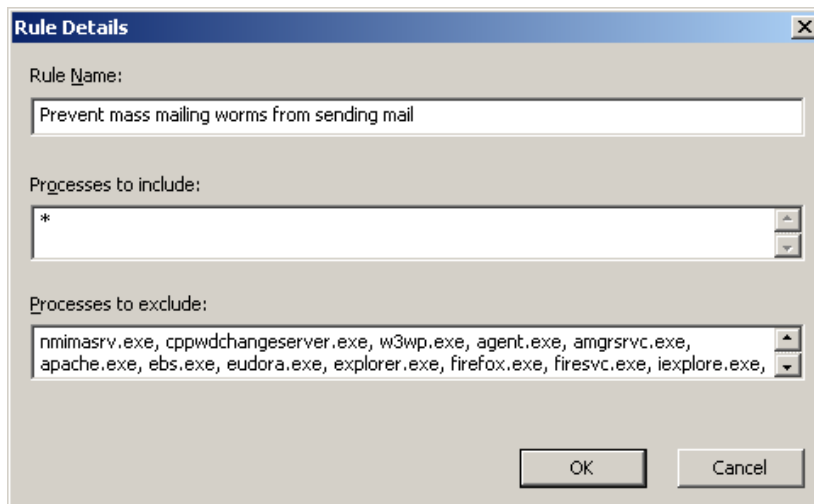
23. Click **OK**.



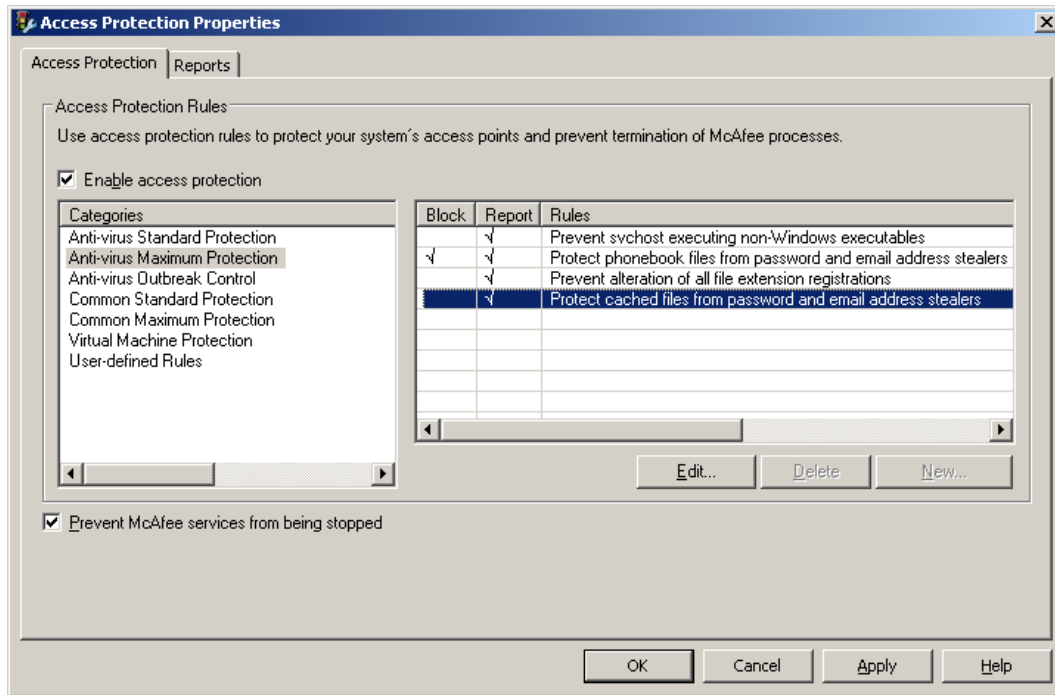
24. On the VirusScan console, double-click "**Access Protection**". On the "Access Protection" tab, select "Anti-virus Standard Protection" on the left. Select **Block and Report options** as shown below. Note: the rules may appear in an order different from shown here. Check the rule text carefully!



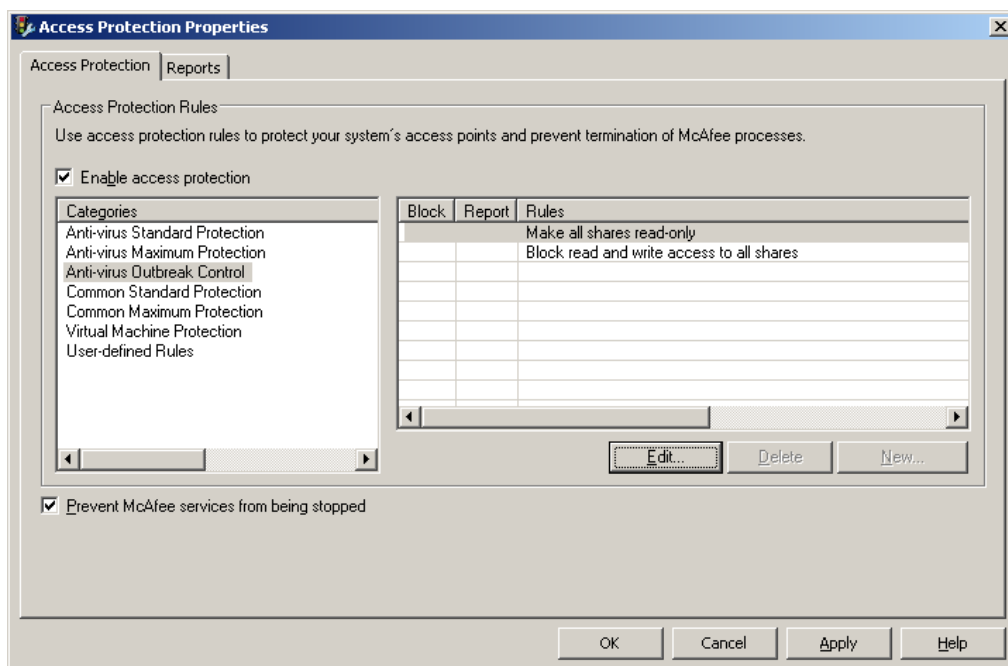
25. Select "Prevent mass mailing worms from sending mail" and click "**Edit...**". Then, under "Processes to exclude", insert "**nmimasrv.exe, cppwdchangeserver.exe, w3wp.exe**" followed by a comma, into the list. Then click **OK**. Note: McAfee sorts this list, so if you later display the list of processes, it will have been sorted alphabetically and nmimasrv will no longer be at the beginning of the list.



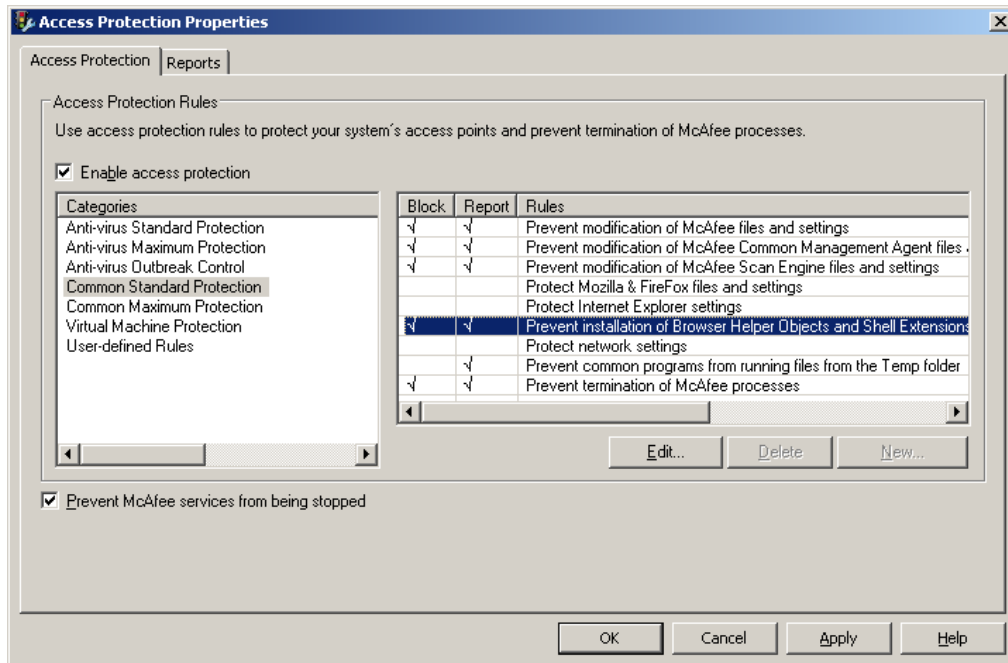
26. Select "Anti-virus Maximum Protection" at the left, then set the **Block and Report options** as shown below:



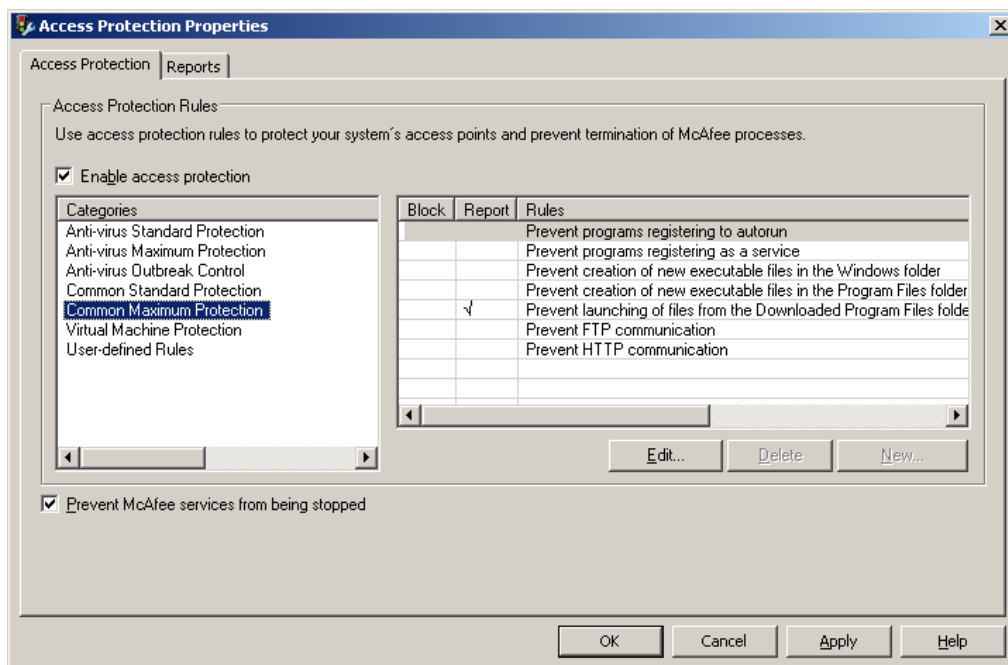
27. Select "Anti-virus Outbreak Control" at the left, then set **Block and Report options** as shown below:



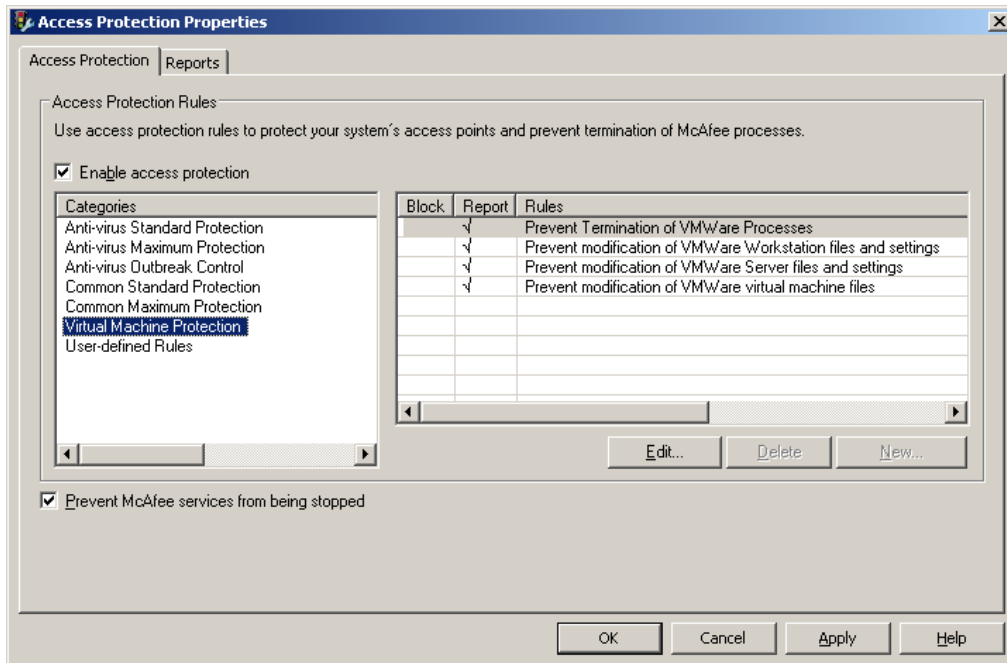
28. Select "Common Standard Protection" at the left, then set **Block and Report** options as shown below:



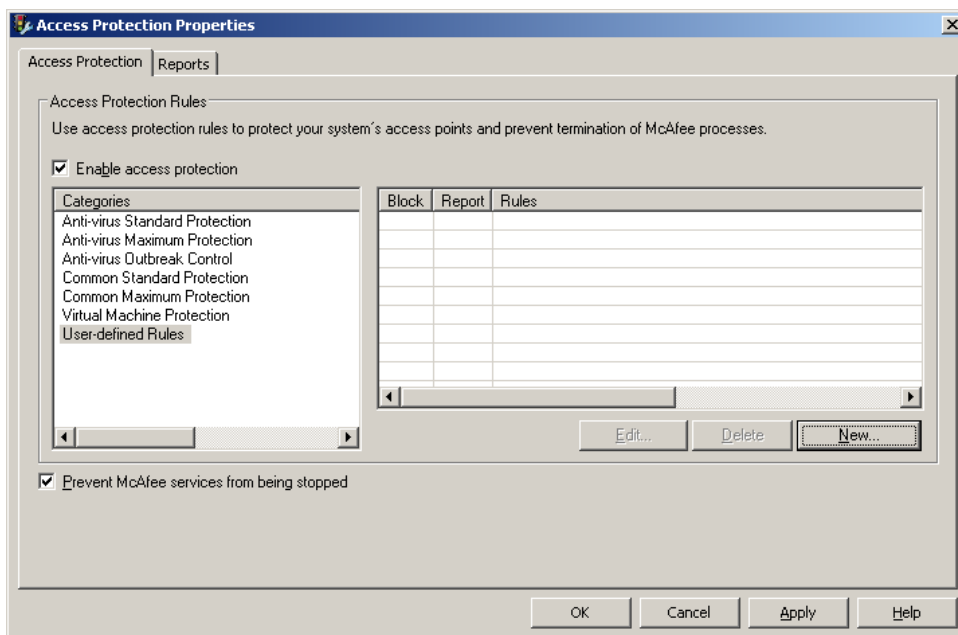
29. Select "Common Maximum Protection" at the left, then set **Block and Report** options as shown below:



30. Select "Virtual Machine Protection" at the left, then set **Block and Report** options as shown below:

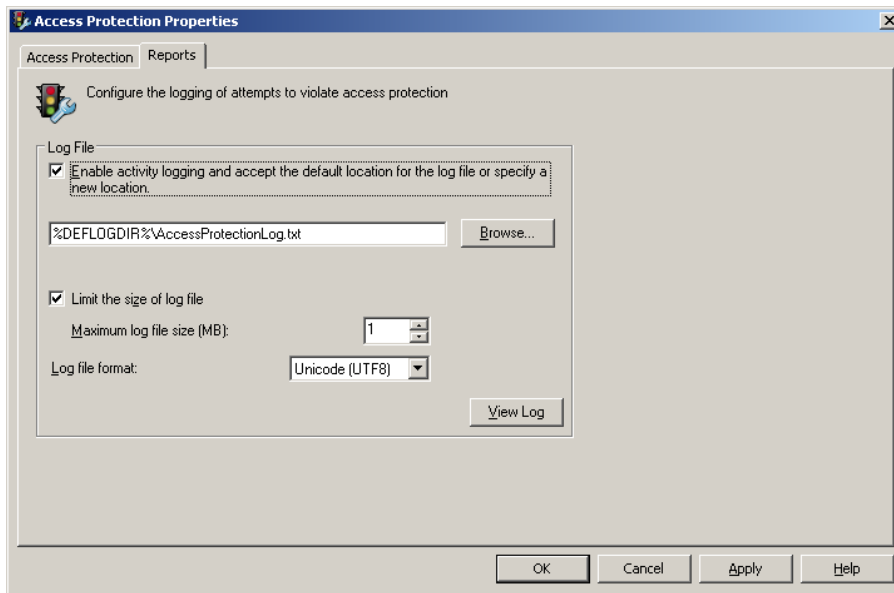


31. Select "User-defined Rules" at the left. There should be **no user-defined rules**, as shown below:

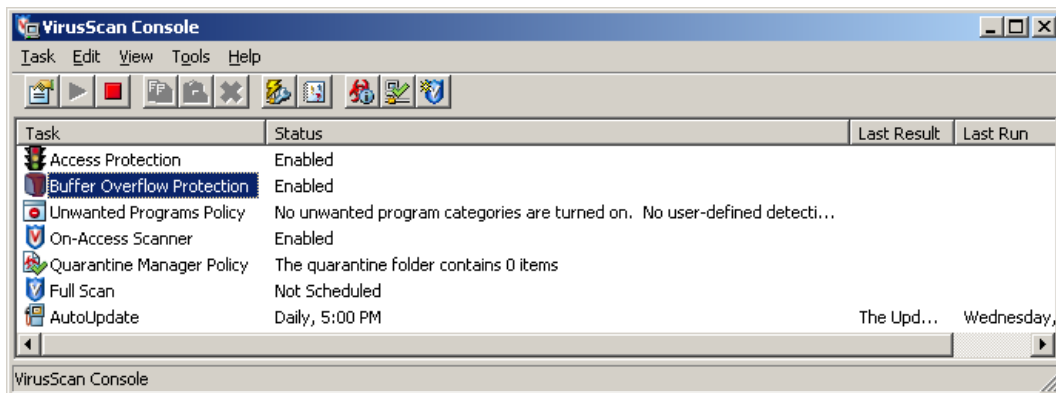


32. Click **Apply** to save all Access Protection changes.

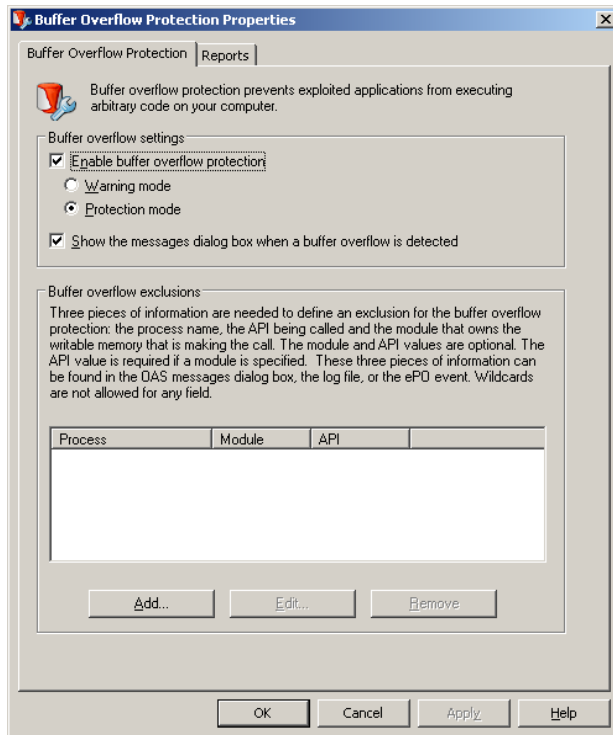
33. Select the "Reports" tab.



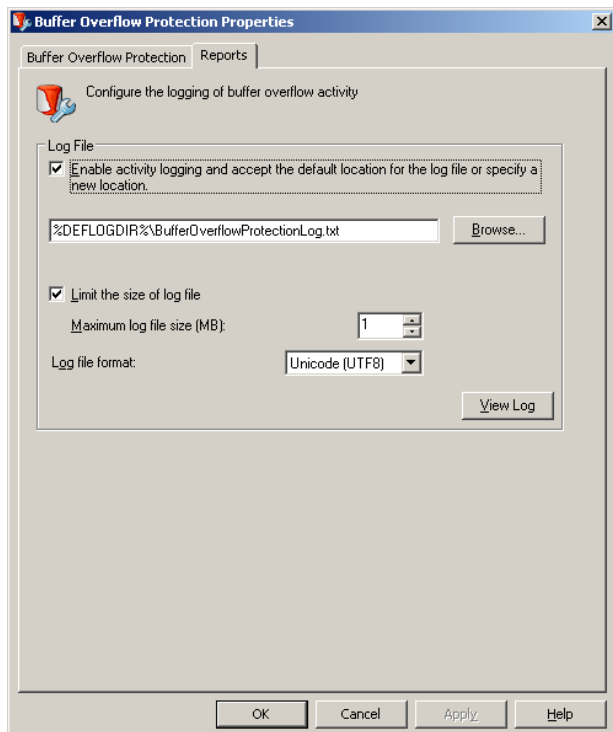
34. Click **OK**.



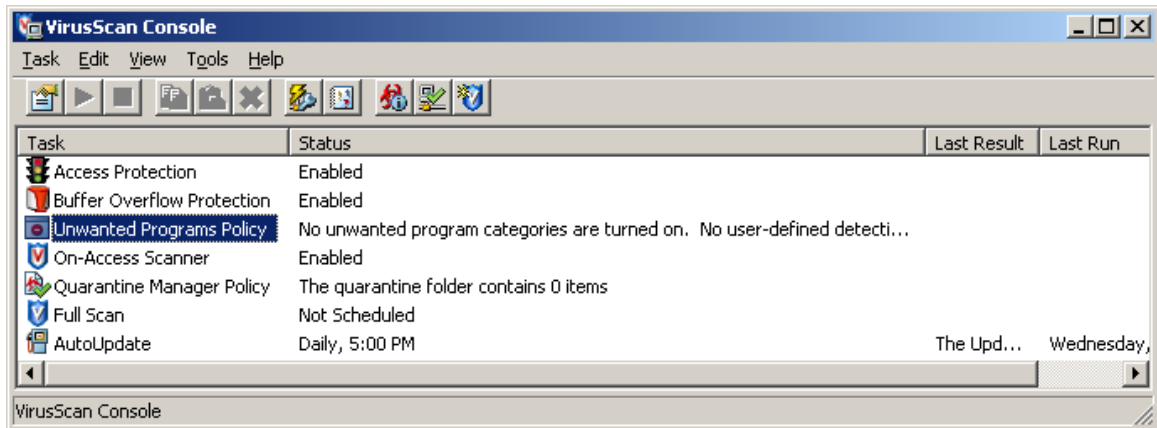
35. On the VirusScan console, double-click "**Buffer Overflow Protection**".



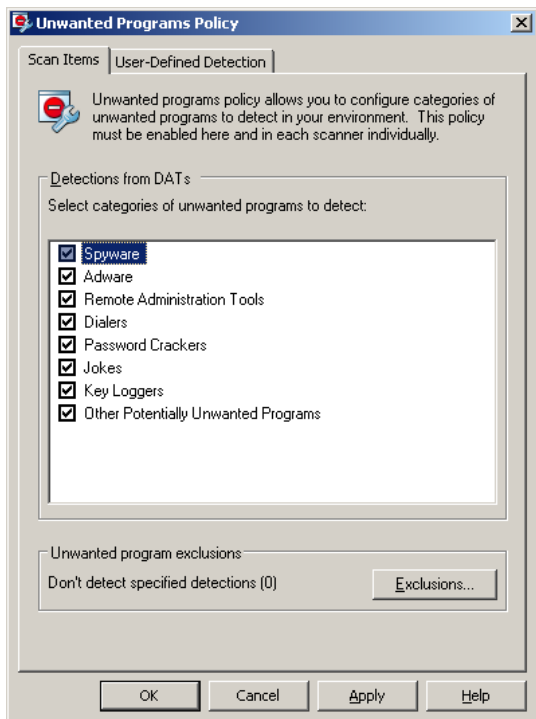
36. Select the "Reports" tab.



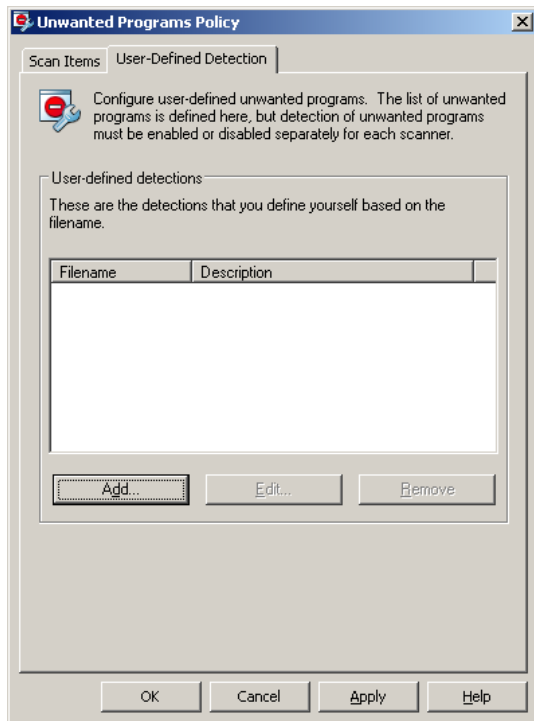
37. Click **OK**.



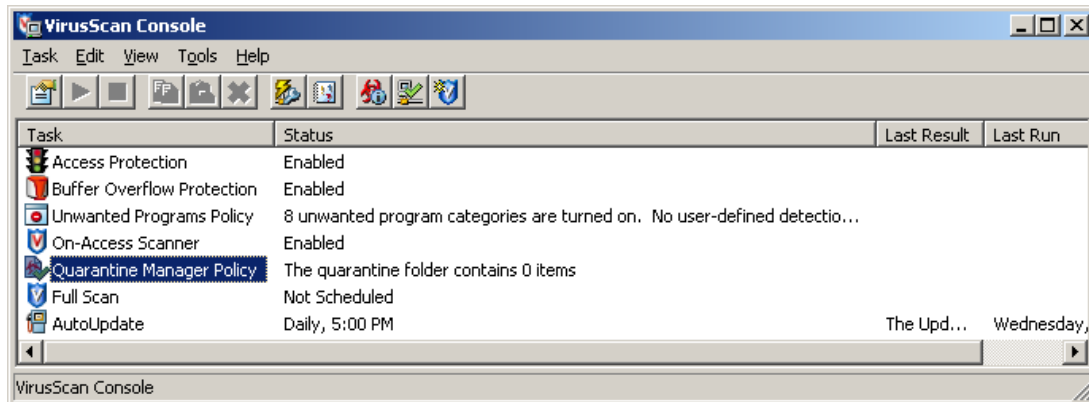
38. On the VirusScan Console, double-click "**Unwanted Programs Policy**" and click to select all checkboxes:



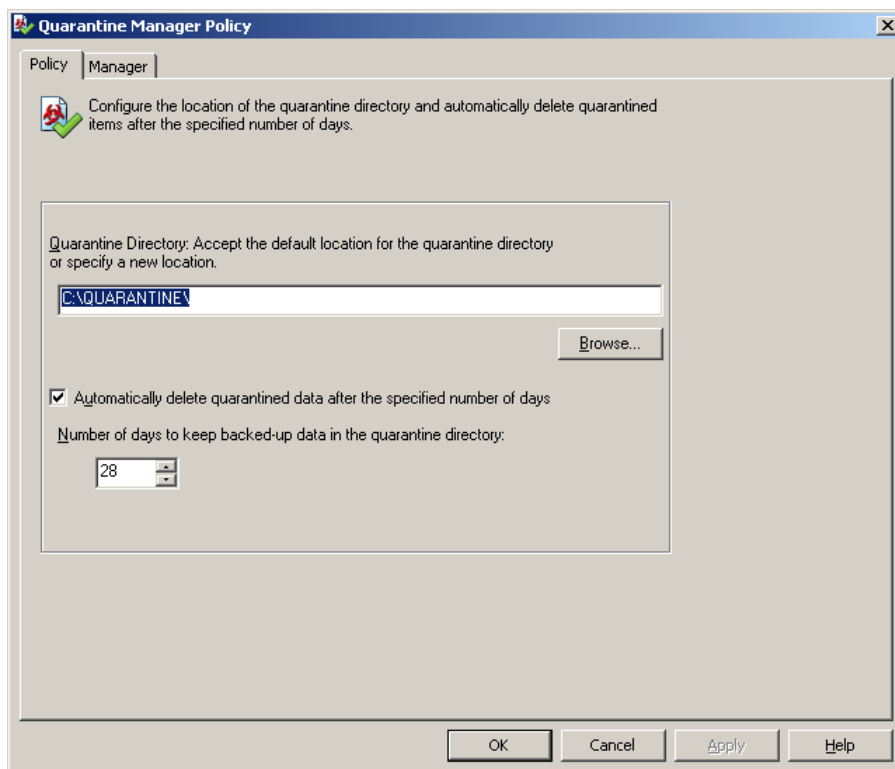
39. Select the "User-Defined Detection" tab



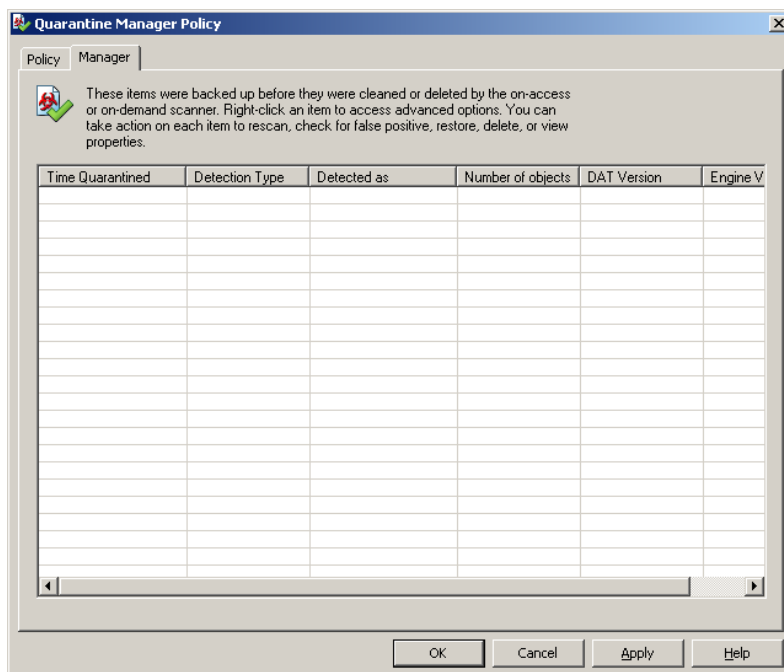
40. Click **OK**.



41. On the VirusScan Console, double-click "**Quarantine Manager Policy**". The Quarantine folder will be C:\Quarantine if the AV software was installed on the C drive (CP5 and later) and D:\Quarantine if the AV software was installed on the D drive (CP4).

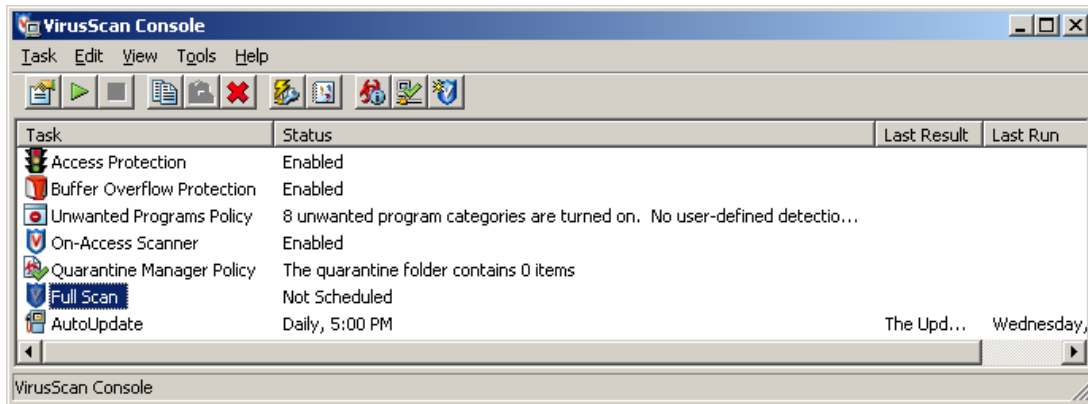


42. Select the “Manager” tab.

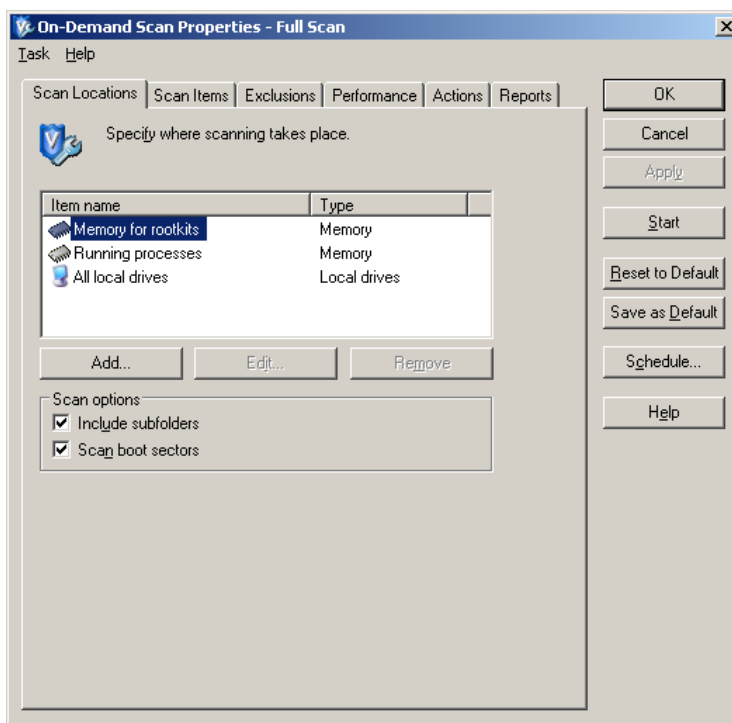


43. Click **OK**.

44. Now run a complete "On-Demand" virus scan to check for any pre-existing infection. The scan may take up to 2 hours on a 201i. (You can skip this step if there is no chance the server could have become infected.) In the VirusScan Console, double-click "Full Scan".



45. Click "Start".

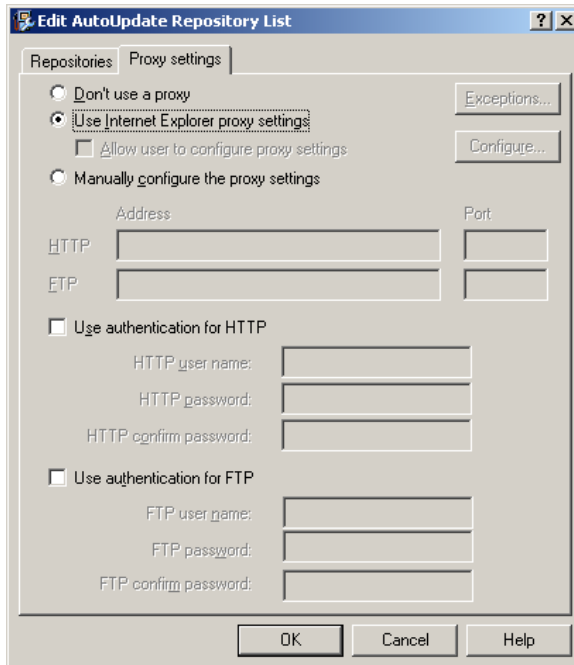


During verification, scan took 1 hr, 5 min on 600r at 100% CPU loading.

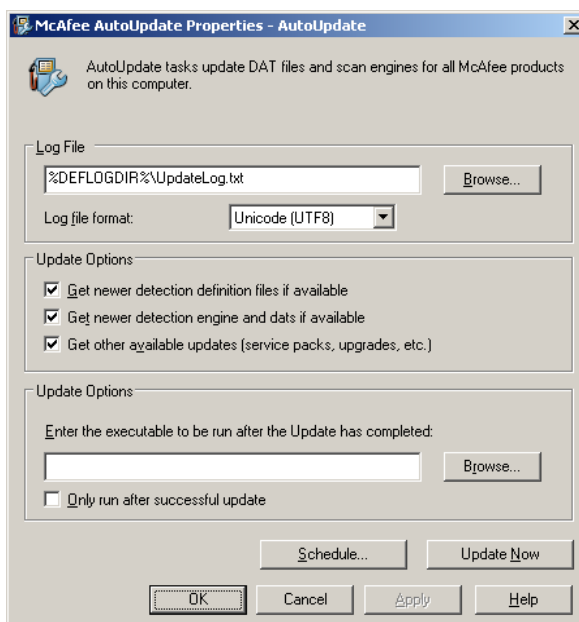
46. If no virus was found on the server, after the scan is completed and you have updated the CallPilot server with the latest OS Security PEPs, you can safely connect the ELAN and CLAN networks.

47. Now configure automatic virus definition updates:

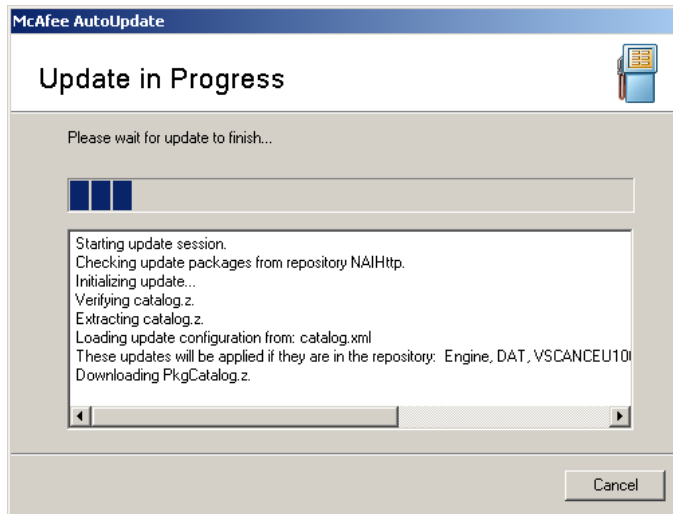
VirusScan Console - Tools - Edit Auto Update Repository List - Proxy Settings tab. The default setting (Use Internet Explorer proxy settings) is likely to be acceptable in order to download definition files directly from the McAfee site. If you are distributing definitions from an internal site, please configure the settings accordingly by consulting the McAfee documentation as needed. Click OK.



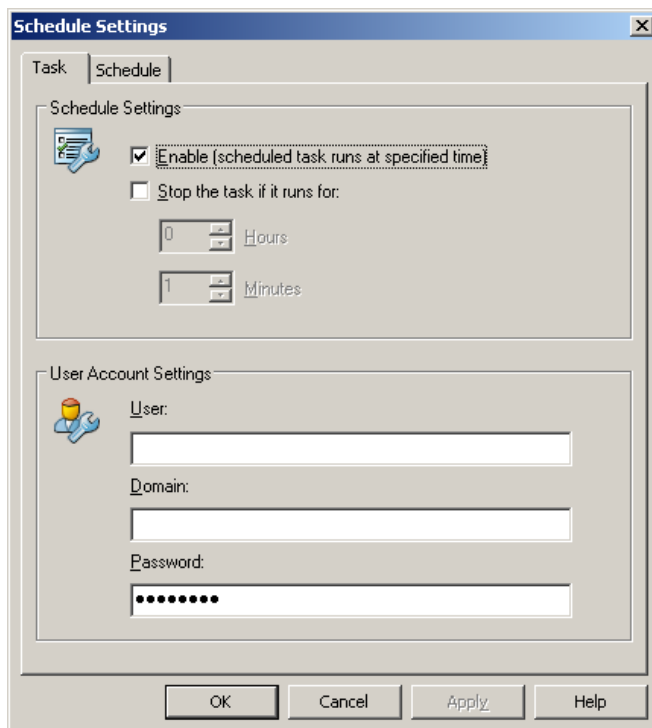
48. On the VirusScan Console, double-click "**AutoUpdate**".



49. Click "**Update Now**" and ensure that VirusScan can access the definition repository. Note that proper configuration of CallPilot CLAN networking parameters, including DNS settings, is necessary for this to work. If the repository cannot be reached, resolve this problem until it works.

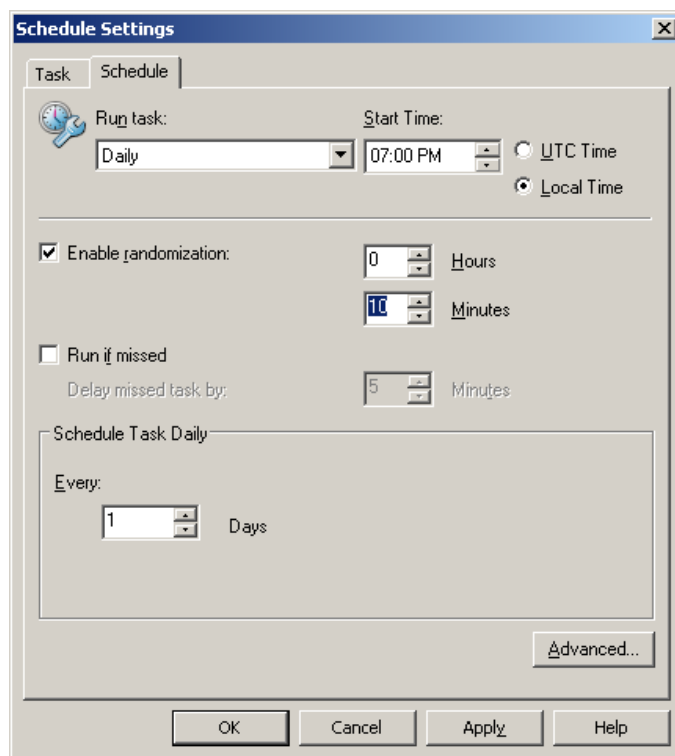


50. The definition update may take quite a long time (over ½ hour) if the definitions have changed greatly since the current definitions. During this time, CPU usage can be very high. Be patient. Once the update has completed successfully, Click the "**Schedule...**" button. Ensure "**Enable (scheduled task runs at specified time)**" is checked.



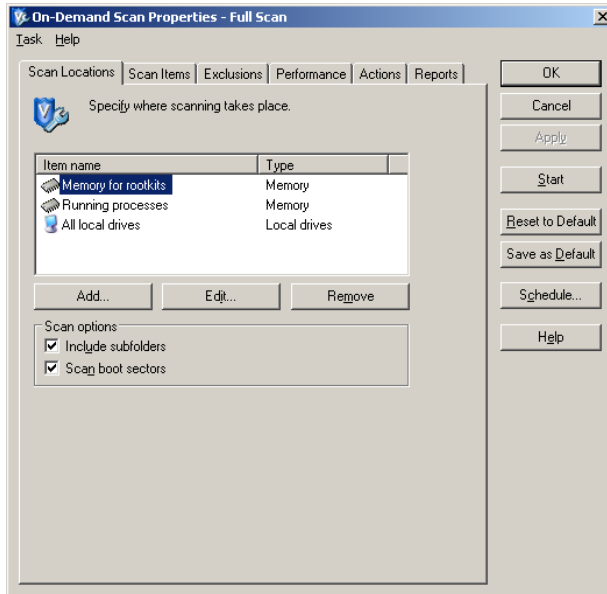
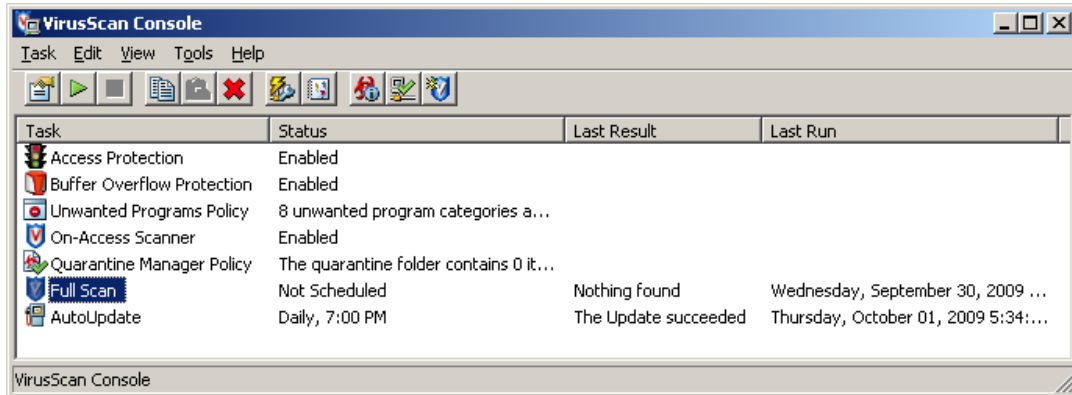
51. Select the "Schedule" tab. Avaya recommends that definitions be updated at least once per week, but no more often than once per day. McAfee releases DAT files every day between 11am and 3pm US Central time. Set the update to occur at a time when system load is expected to be very low to ensure that normal CallPilot server operation is less likely to be impacted – the evening is usually a good time. It can take up to 20 minutes to update the definitions.

Note: If you plan to set up a regular scheduled virus scan, it is a good idea to coordinate the update time so that the update process will be complete prior to the scheduled scan so that the scan is carried out using the most up-to-date definitions. Uncheck the box **"Run if missed"** (Otherwise, this could result in the operation being done at a bad time.) Set the randomization interval to 0 hours, 10 minutes.

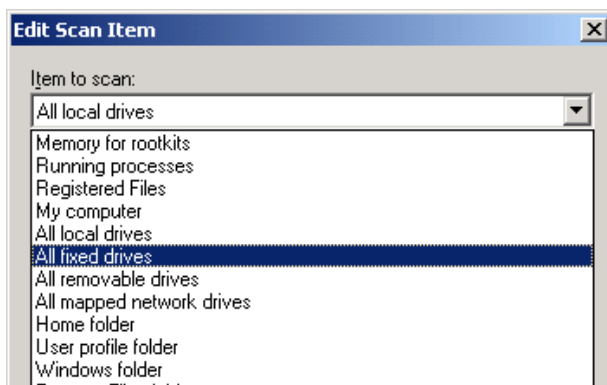


52. Click **OK**. Click **OK**.

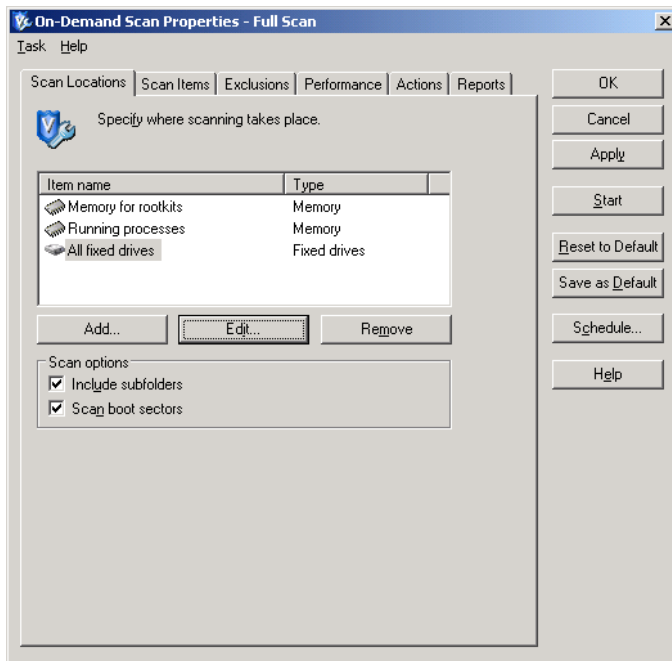
53. Now configure a periodic, scheduled full virus scan. On the VirusScan Console, double-click **"Full Scan"**.



Click to select **"All local drives"** and click **"Edit..."**.



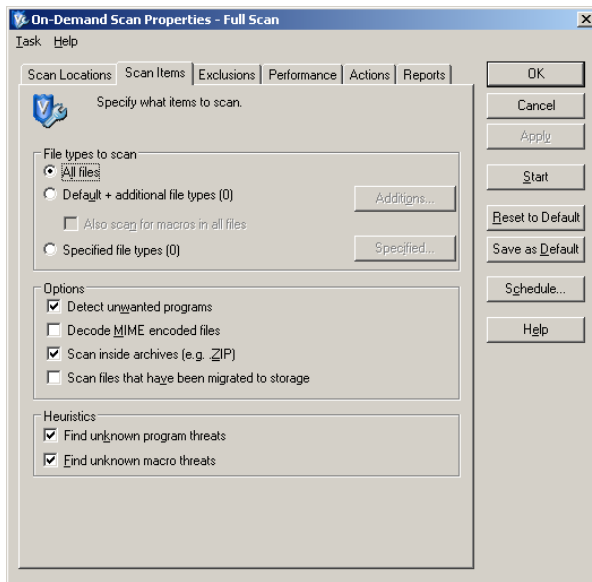
In the “Edit Scan Item” window, select “**All fixed drives**” in the drop-down box. This will cause all hard drives to be scanned, but VirusScan will not scan removable drives. Otherwise, if an error occurs reading a CD or floppy disk, the AV scan or even CallPilot operation might be impacted. Also the time needed for a full scan could increase significantly. Click **OK**.



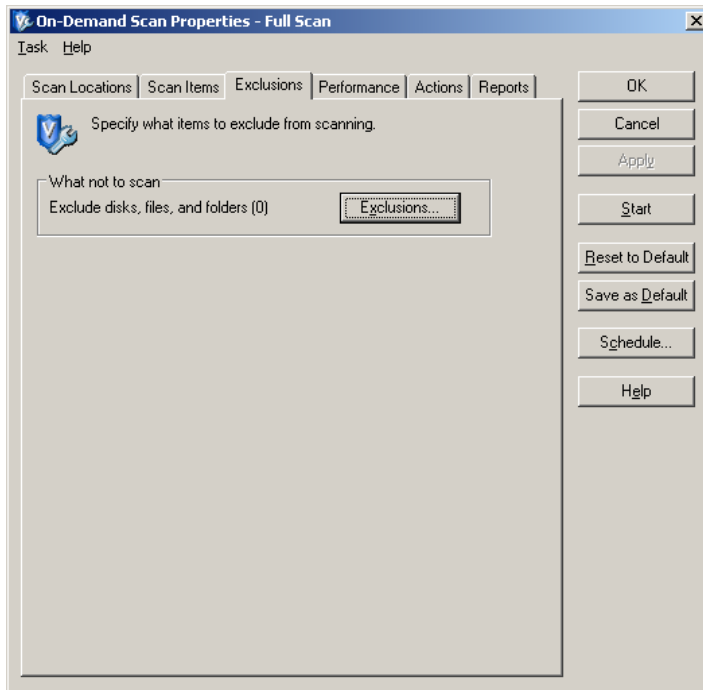
These guidelines will show how to set up a full virus scan every week. This full scan of all local drives will take many hours and will have a significant performance impact on CallPilot, therefore it must be done during off-hours, e.g. on a weekend.

McAfee also allows memory-only scans ("Memory for rootkits" and "Running processes") to be scheduled, without scanning local drives. In addition to a periodic full local drive scan, the customer may choose to perform more frequent memory-only scans (e.g. daily) -- these take less time (approx 2-5 minutes) and have less system impact, however they still should be done only at off-peak hours.

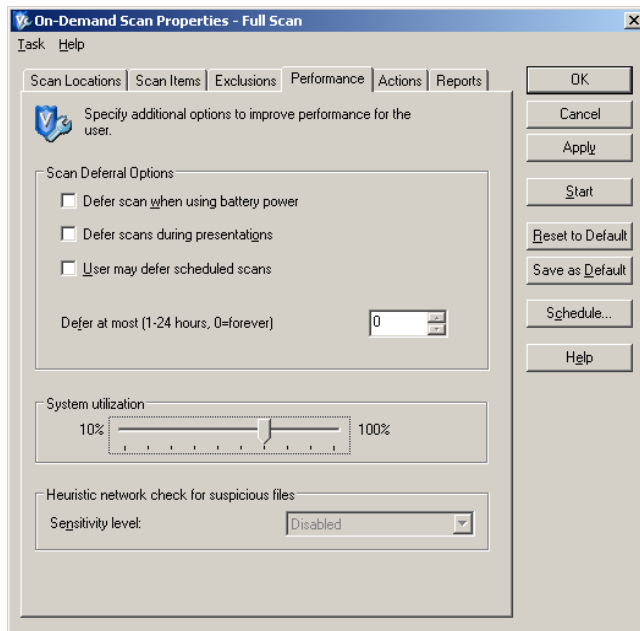
54. Select the "Scan Items" tab.



55. "Exclusions" tab -- no exclusions are required for the on-demand scan.

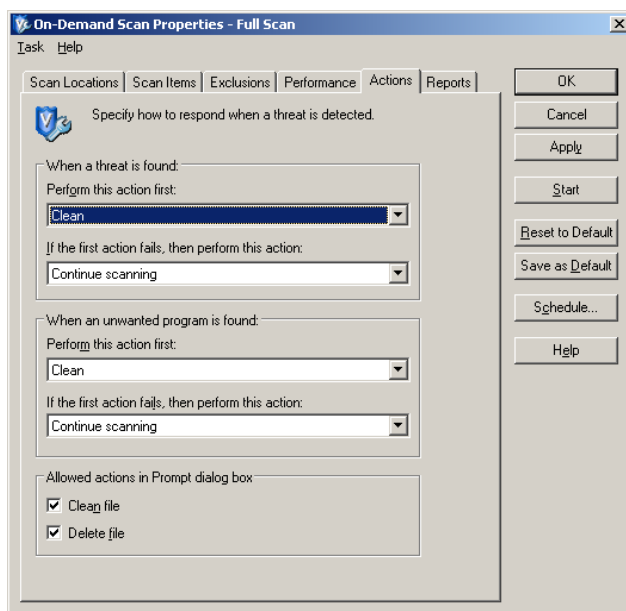


56. Select the "Performance" tab.



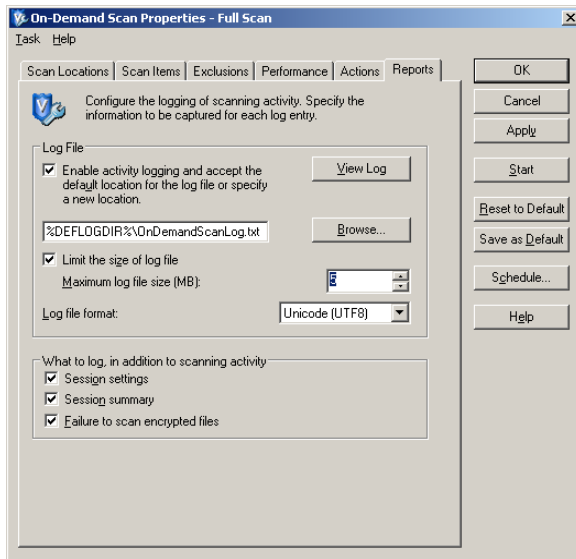
57. Click and drag the "**System utilization**" slider to the **70%** mark (4th tick from the right). (A complete AV scan on a 201i will take about 4.5 hours with this setting, assuming D:\TEMP is clear. Setting a lower percentage will cause it to take longer -- which could be problematic. Setting a higher percentage could result in poor response time for any callers who access the system during the scan.) NOTE: even with this set to 70%, the scan32.exe process seems to consume over 90% of the system CPU during a full scan.

58. Select the "Actions" tab.



59. Under "When a threat is found", under "If the first action fails...", select "**Continue scanning**". Under "When an unwanted program is found", under "If the first action fails...", select "**Continue scanning**".

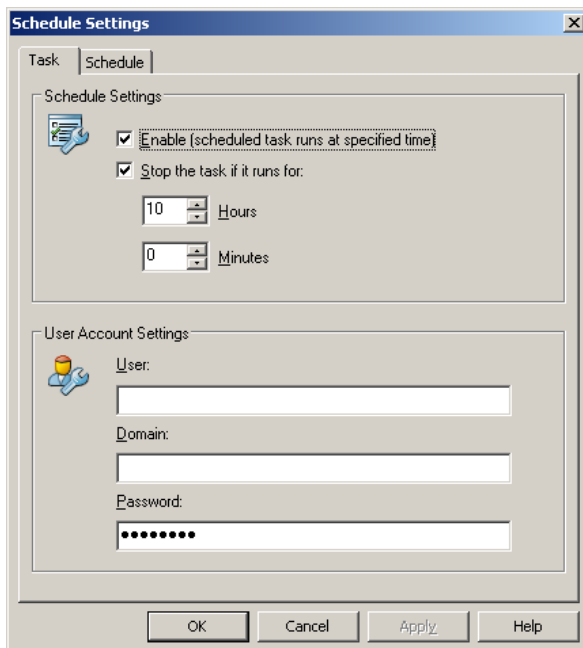
60. Select the "Reports" tab



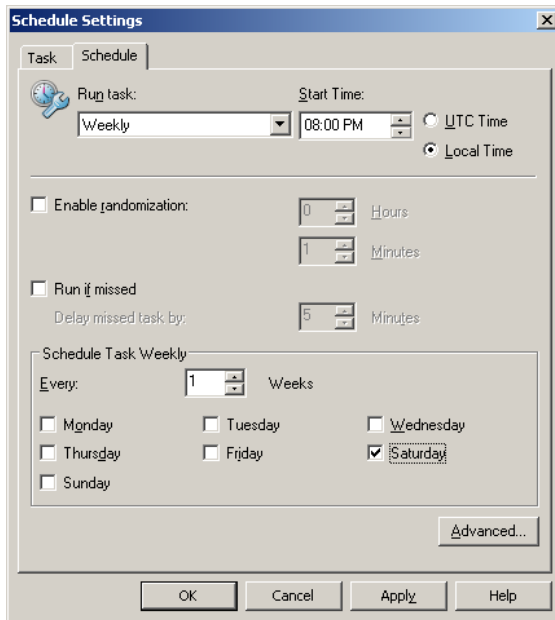
61. Set the maximum log file size to **5 MB**. Check the box "**Session settings**".

62. Click **Apply** to save all the on-demand scan properties.

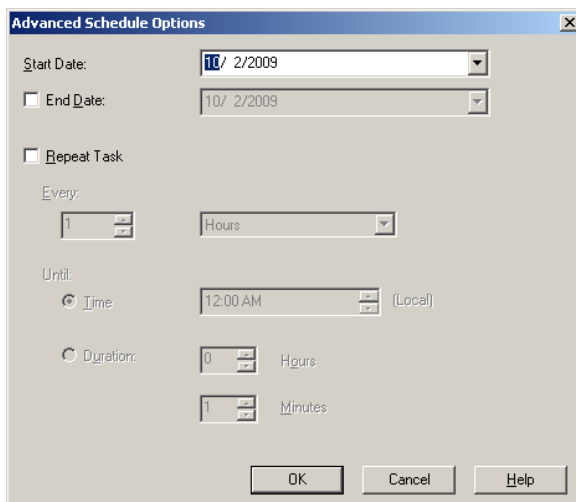
63. Click "Schedule..."



64. Select "**Enable (scheduled task runs at specified time)**". (You may, optionally, also set a time limit here to ensure the scan is terminated before a busy time period -- the time limit should be chosen according to when the scan is being scheduled and when traffic is expected to ramp up.)
65. Select the "Schedule" tab.



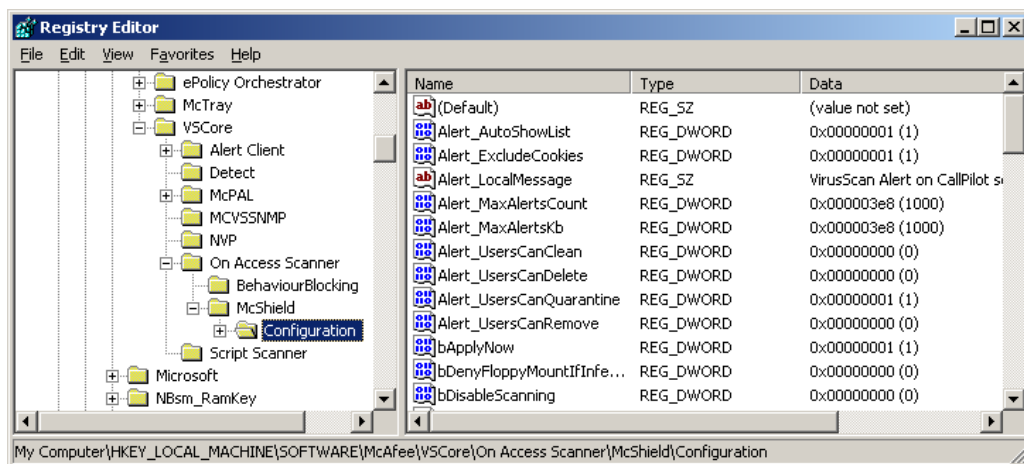
66. Pick a time for the scan when the load on the CallPilot server is expected to be low for the duration of the scan. Scans can be done daily, every few days or weekly. The day of the week can be selected.
67. If you click the "Advanced" button, you will see options to end scanning at a specified date or to repeat the task periodically. Neither of these options are recommended for CallPilot.



68. Click **OK**. Click **OK**. Click **OK**.

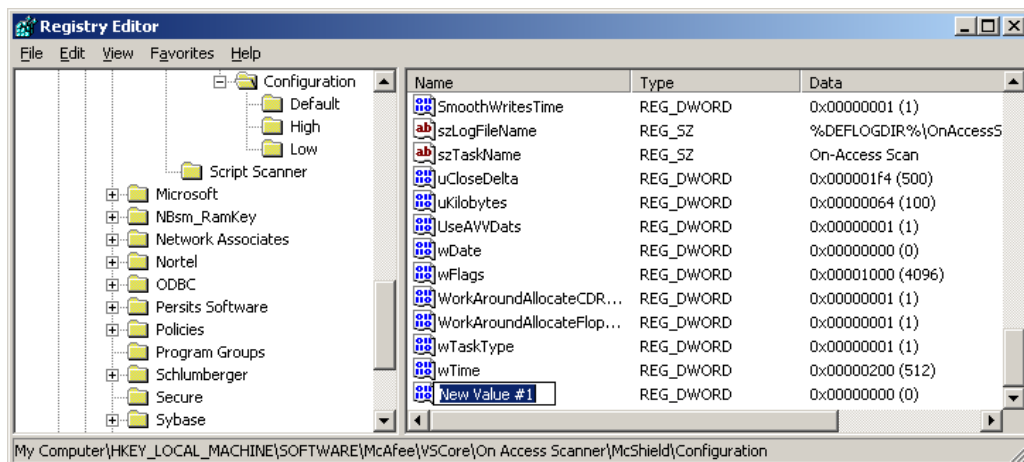
69. Now we must configure a workaround to that the McShield on-access scanning process runs at normal priority rather than high priority. (Otherwise, the McShield process can starve CallPilot application processes of CPU for many seconds under certain circumstances – this can result in a system outage that may not be recovered automatically.)

70. First, temporarily disable Access Protection. On the VirusScan Console, right click Access Protection and select "Disable". (otherwise the registry change needed will be blocked by the Common Standard Protection rule "Prevent modification of McAfee files and settings".) NOTE: use care when updating the registry.

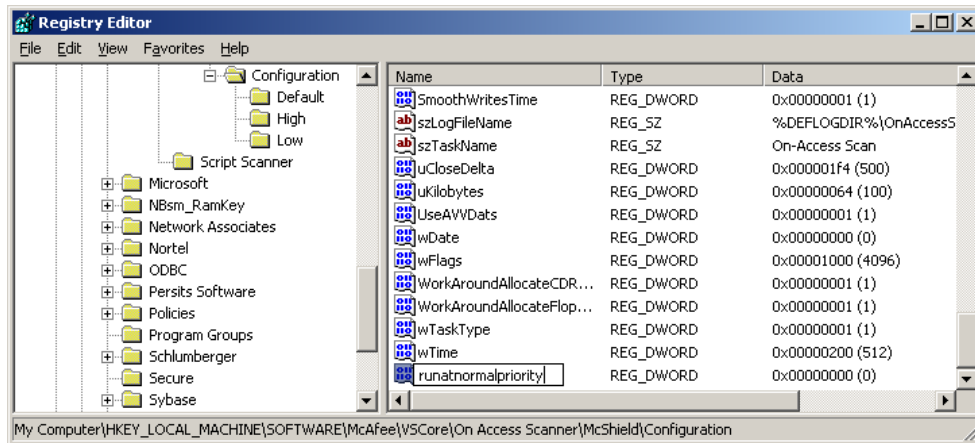


71. Start - Run, type **regedit.exe**. Browse to My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\VSCore\On Access Scanner\McShield\Configuration.

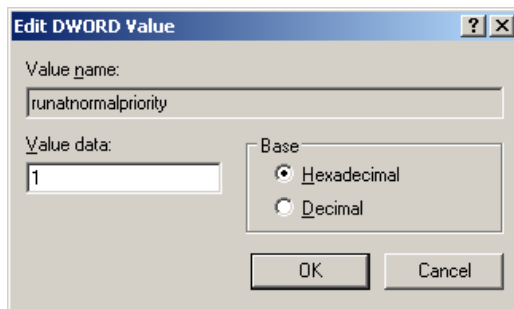
72. With the "Configuration" key selected, under the "Edit" menu, select "**New**", then "**DWord** value".



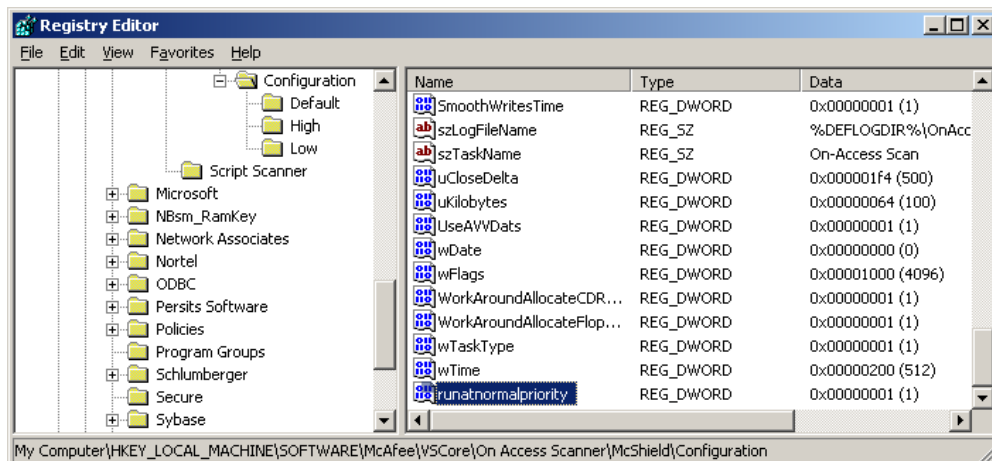
73. Replace the text "New Value #1" with "runatnormalpriority".



74. Double-click the new value and set it to 1.



75. Click **OK**.



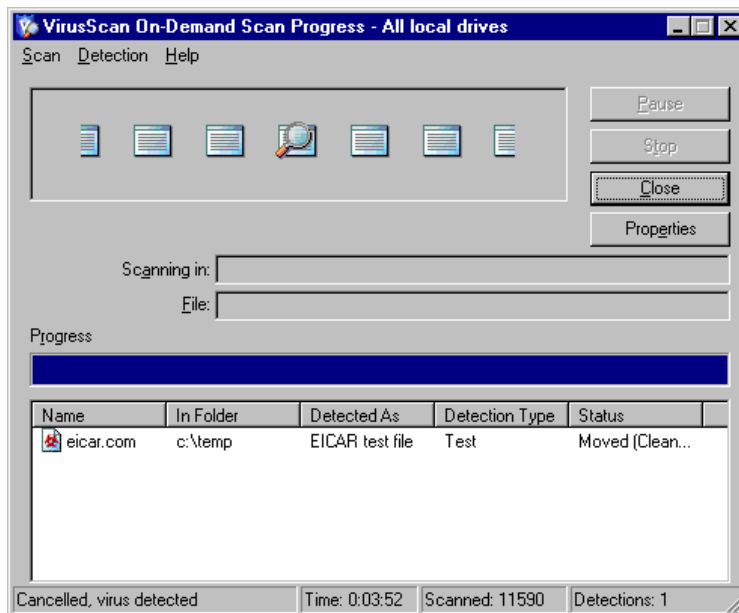
76. Close regedit

77. Now re-enable Access Protection. On the VirusScan console, right click Access Protection and select "Enable".

Testing

Once you have configured McAfee VirusScan, you should test that it works. Of course, you do not want to use a real virus. There is a "test virus" available for download from <http://www.eicar.org>.

This is not a real virus, however it is detected as one by your antivirus software. This allows you to check the proper configuration of your virus protection and alerting. Also, you should periodically check to ensure that virus definitions are being properly updated automatically.



Issues that may be encountered

Services not starting after reboot.

When a CallPilot server reboots, many CallPilot services must start up. Multiple McAfee processes also start up, initialize themselves and start running after a reboot. After being started, a CallPilot service must respond within a 30 second timeout. On less powerful servers (e.g. the 201i), one or more CallPilot services might not start up automatically. McAfee seems to create some additional system load during the startup period resulting in services taking longer to start up.

This problem seems to occur most often in the initial reboots following McAfee installation and definition updates. Once the system is fully initialized and updated, the problem seems to happen less frequently.

If a given service does not start, it can be started manually using the Windows Services applet.

If the problem persists, here are a few things to try (these have not been proven to solve the problem, however):

1. Try defragmenting the C and D partitions. (Windows Explorer, select drive, right-click Properties, Tools tab). This may speed up program loading slightly
2. Wait before logging in at the Windows console. Logging in during system bootup just adds even more load and slows startup down even more.

Full Scan takes too long

On certain CallPilot platforms (e.g. the 201i), a full anti-virus scan can take many hours. The scan needs to be scheduled so it completes before CallPilot traffic increases the next morning. If the scan takes too long, it may be difficult to find a low traffic period long enough to allow the scan to run.

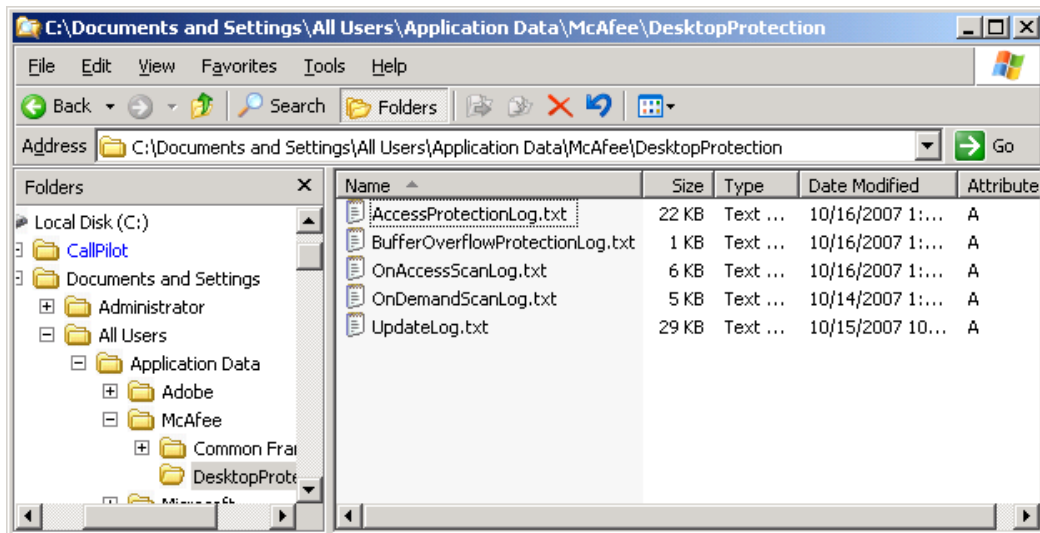
1. Remove any unneeded large temporary files. For example, large CallPilot PEPs are often saved under D:\TEMP or on the desktop (of any of the Windows usersids). These tend to be large compressed files that take a long time to scan. Delete any such files that are not needed.
2. If large files must be retained, define exclusions in the full scan to avoid scanning them (see the screen for step 55 above).

CallPilot slow performance

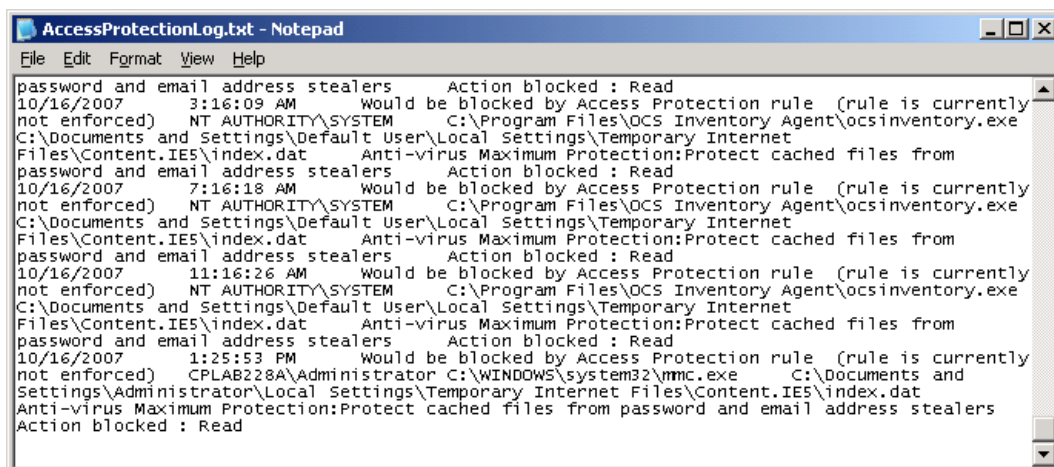
1. Using Start – Programs – Administrative Tools - Local Security Policy check under Security Settings – Local Policies – Audit Policy. Ensure that “Audit Privilege Use” is set to “Failure” and is not set to “Success, Failure”. (This audit can result in slow performance for hours or days following an AV scan since it results in a very large number of security event logs that need to be generated and processed.)
2. Check that an AV scan or a definition update is not active.

VirusScan Log Files

By default, VirusScan log files are stored on the C drive, in the folder shown below:



The operation of the Access Protection feature is shown in the AccessProtectionLog.txt file as shown below. The “V” tray icon at the bottom right of the Windows desktop will have a red background if something gets written to the AccessProtection log file.



Log files are also maintained for BufferOverflowProtection, OnAccessScan, OnDemandScan and definition Updates. Please consult the McAfee log files if problems are suspected with the McAfee program. Also, VirusScan generates event logs in the Windows Event log. (Look for source “McLogEvent”). It is normal for scanning to fail on file “mctools.exe” since this is an encrypted archive.

Definition updates pushed from ePO don’t show up in the UpdateLog file. Look in the Windows Application Event log for McLogEvent 5000. This gives the new DAT file number.

ePolicy Orchestrator (ePO)

McAfee's ePolicy Orchestrator product provides the ability to manage security defenses on a whole network of computers from a single management console. Many large CallPilot customers use tools like this to conveniently control the security of large numbers of desktop PCs and other computers on their network.

When a CallPilot server is managed via ePO, several issues may arise:

- Incorrect configuration options may be applied to the CallPilot server. This can result in CallPilot service problems including system outages
- Unauthorized software (e.g. McAfee AntiSpyware) may be mistakenly deployed to a CallPilot server
- Virus definition updates may be pushed to the CallPilot server at an inappropriate time such as during busy times.
- Typically the Avaya and partner personnel supporting the CallPilot equipment will not have access to the ePO console and therefore must rely on cooperation from the customer's IT organization.
- The user interface for specifying VirusScan configuration parameters is somewhat different in ePO from that used by the VirusScan console.

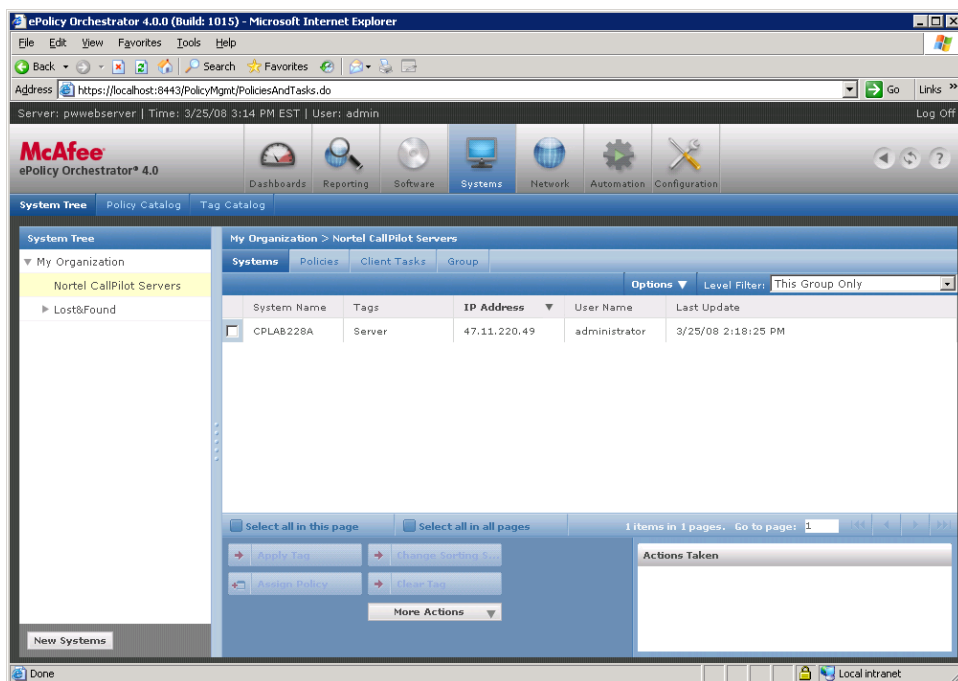
A full discussion of how to use ePO is beyond the scope of this document. However, some information is given here to help ensure that CallPilot servers are properly treated under an ePO framework. Refer as needed to the McAfee ePO documentation.

Different versions of ePO exist. ePO 3.5 uses an interface based on Microsoft's MMC (Microsoft Management Console). ePO 4.0 uses a web-based interface within a browser. Either version can manage various versions of McAfee products running on a variety of OS platforms. ePO 4.5 is now available – it is mostly similar to 4.0.

The screenshots here are from ePO version 4.0.

Typically, a customer's network will contain a large number of desktop PCs and a variety of servers of different types. The customer's IT organization will usually have some anti-virus policies that they have standardized on for their desktop PCs. They may also have defined policies for some of their server computers. CallPilot servers have specific requirements (as detailed in this document) for how VirusScan needs to be configured. Therefore it is necessary to define CallPilot servers separately within ePO. Under no circumstances can policies intended for desktop PCs be applied to a CallPilot server.

A customer may have multiple CallPilot servers on their network. Within ePO, it is possible to create a "subgroup" under "My Organization" and move the CallPilot servers to that group as shown below:



It is also possible, instead of using a group or subgroup, to manage the VirusScan settings on a per-computer basis.

An ePO policy can be set up for “workstations” or “servers”. Be sure to always select “server” for the CallPilot server.

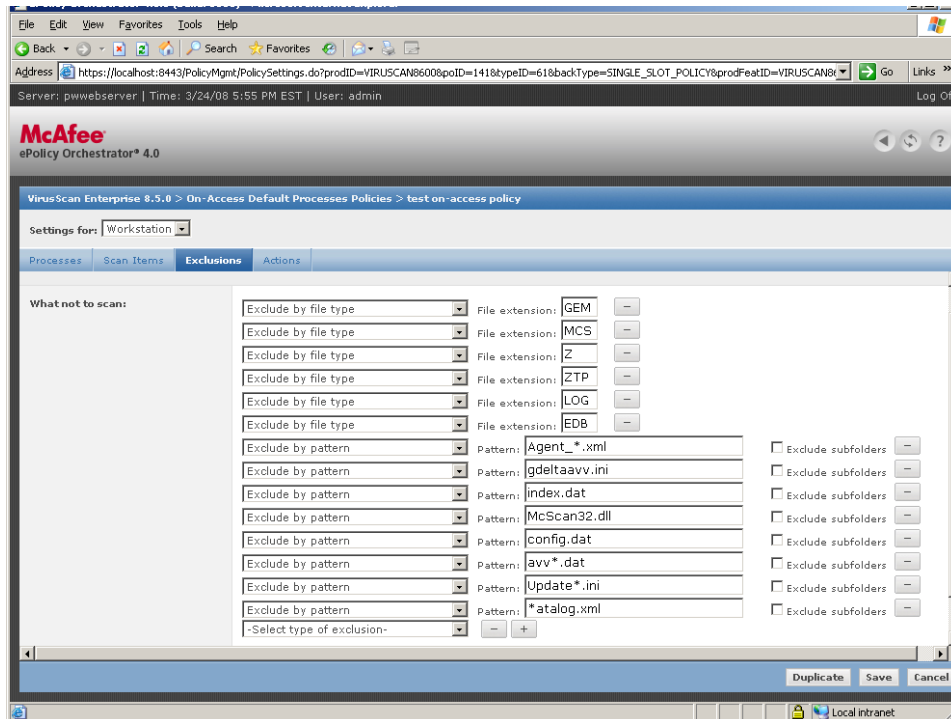
In ePO, VirusScan settings are, by default, inherited hierarchically from higher levels in the hierarchy of computers on the network. Ensure that incorrect settings are not accidentally inherited by selecting “Break inheritance” for every policy.

Within ePO, there are separate “categories” of settings: e.g. on-access scanning, access protection, unwanted programs. For each category, a policy (ePO 4.5 calls them “assigned policies”) can be defined for the settings within that category. Create a separate policy for CallPilot for each of the categories. Initialize that policy by duplicating the McAfee default, then adjust the policy to conform to this document.

Scheduled activities, such as on-demand scans or definition updates are defined using “Tasks”. Define tasks for these activities for CallPilot servers – be sure to specify “server” and not “workstation” for these tasks in the drop down box in the upper left of the screen.

In order to avoid CallPilot service outages when virus definition updates are performed, it is important to only do definition updates at periods of low CallPilot traffic, to ensure that VirusScan Patch 4 or later is installed and to ensure the On-Access Exclusions have been properly set up on the CallPilot server (configuration step 6 above).

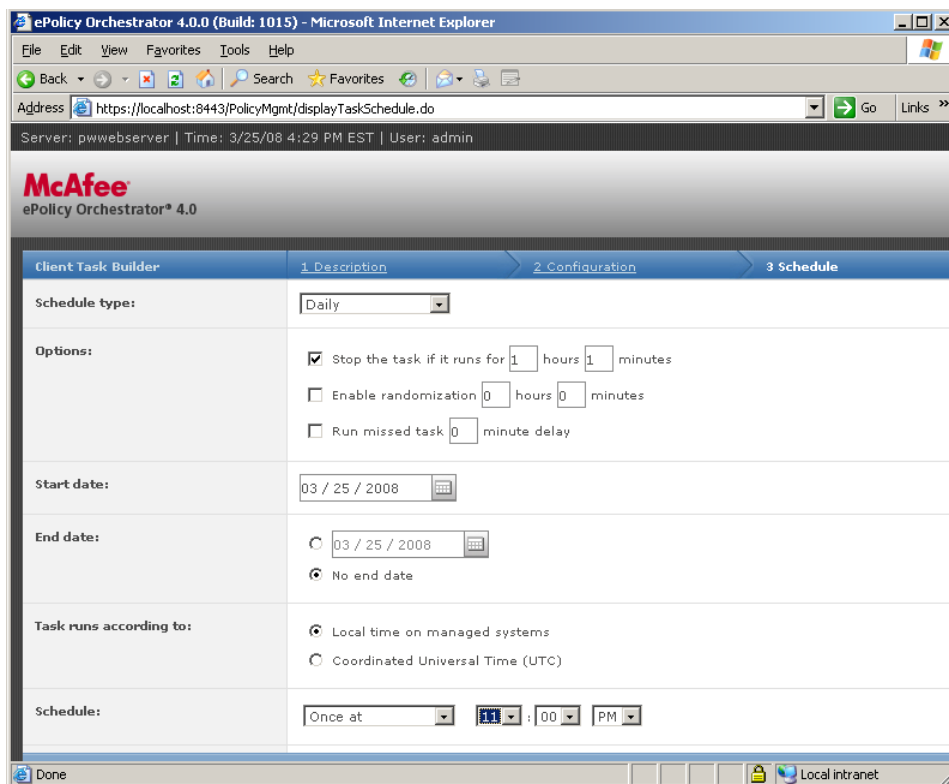
When VirusScan configuration is specified using ePO, the user interface is different from the local VirusScan console. Here is a screenshot from ePO 4 showing on-access scanning exclusions set up as required for CallPilot servers:



Access Protection can also be configured within ePO. For the "Anti-Virus Standard Protection" settings (see configuration step 16 above), a "process to exclude" must be added so that CallPilot network message transfer still works.

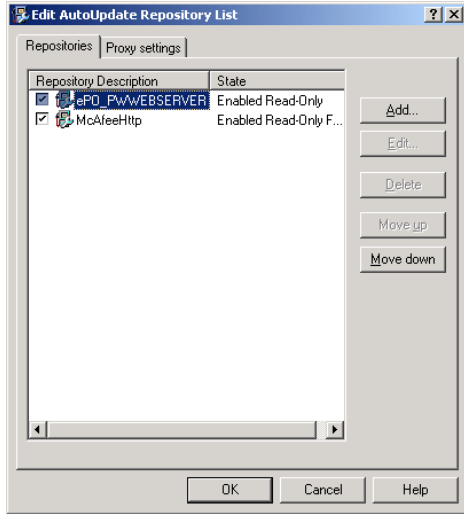
The ePO agent may be installed and working on a CallPilot server but it may not show up on the client PC's Add/Remove Programs list

Via ePO, "Client Tasks" can be used to update definitions. These can be scheduled. It is possible to schedule them to run repeatedly during a given time interval, at an interval given in hours or minutes. Be sure to schedule definition updates to CallPilot servers only for times the CallPilot server is expected to have very light traffic loads.



Client tasks can be created to deploy additional software, for example, the "AntiSpyware Enterprise Module 8.5.0". Note that the AntiSpyware module is not authorized for use on CallPilot servers and must not be deployed onto CallPilot servers.

Even though it is not obvious that the ePO agent is installed on a CallPilot server, it is still possible that virus definition updates are being pushed to the server, possibly at inappropriate times. In VirusScan console, under the "Tools" menu, select "Edit AutoUpdate Repository List". This may show an ePO repository. There is nothing wrong with obtaining definitions from such a repository as long as those definition updates occur only during periods of very low CallPilot usage. Otherwise CallPilot service may be affected.



When configurations are being specified using ePO, be sure to check the settings on the local CallPilot VirusScan console to ensure the correct settings have been set. Any incorrect settings will need to be corrected on the ePO side. (If you simply change them locally, ePO will overwrite with the centrally specified policy at the next policy enforcement).

McAfee VirusScan 8.7 Resource Usage

McAfee Processes and Observed Memory usage (ePO agent not installed):

Process	Description	Typical Virtual Memory Usage during normal CallPilot execution	Maximum Memory Usage Observed
CmdAgent.exe	CMA Command Line Processor	0	
Csscan.exe	Command line scanner	0	
EngineServer.exe	McAfee Engine Server	664 KB	
Entvutil.exe	Buffer Overflow Protection Rule File Update Utility	0	
FrameworkService.exe	Framework Service	5.3 MB	5.5 MB
Frmlnst.exe	CMA Setup Program	0	
Logparser.exe tool	Logparser reboot notification	0	
Mcadmin.exe	VirusScan Vista admin process	0	
Mcconsol.exe	VirusScan Console	0	11 MB
McScanCheck.exe	McAfee Agent McScan Check	0	
McScript_InUse.exe		0	260 MB during def update
Mcshield.exe	On-Access Scanner service	44 MB	122 MB
Mctray.exe	McAfee Security Agent Taskbar Extension	500 KB	
McUpdate.exe	VirusScan AutoUpdate	0	1.9 MB
Mfeann.exe	VS Core Announcer	2 MB	2.1 MB
Mfehidin.exe	Host Intrusion Detection Driver Installer	0	
Mfevtps.exe	McAfee Process Validation Service	3.4 MB	3.5 MB
Mytilus3_server_process.exe	Common Shell3 – Scanner's Interface to the 5000 Series Engine	0	
naPrdMgr.exe	NAI Product Manager	3.8 MB	3.9 MB
NCInstall.exe	Installer for McAfee Notes Scanner	0	
Pireg.exe	Checkpoint Software Technologies	0	
Restartvse.exe	Restart Support module for VSE	0	
Scan32.exe	VirusScan On-Demand Scanner	0	149 MB during scan
ScnCf32.exe	VirusScan On-Demand Scan Task Properties	0	
Shcfg32.exe	Shield Config Properties	0	
Shstat.exe	VirusScan Tray icon	2 MB	2 MB
UdaterUI.exe	Common User Interface	3.9 MB	
VSTskMgr.exe	Task Manager	7.6 MB	8.7 MB

Appendix-D

This appendix provides Installation and Configuration procedures for CallPilot 4.0 and 5.0 servers utilizing the **Symantec EndPoint Protection 11** anti-virus application.

Product Features

- Performs memory, boot sector and disk scanning. Good management features.
- In addition to anti-virus, now includes anti-spyware, firewall and intrusion prevention features, all manageable from a central management console
- Has capability of repairing root-kits
- Virus definition updates occur even when the console is logged off.
- Virus definition update does not significantly impact CallPilot performance

Product Deficiencies

- Reboot may be required after install/update
- No Proactive Detection feature on Windows Server 2003, but it seems to update it anyway.
- Consumes significant CPU for firewall protection even when no load on system (~15% on 201i). Not installing Network Threat Protection only slightly reduces this cost. Other AV products are a better choice in cases where a system is running at the maximum capacity allowed for the hardware platform.
- Consumes a lot of disk space on the C drive, even when the product is installed on the D drive.
- Product versions prior to MR4 have resource utilization bugs and are not authorized for installation on the CallPilot 201i IPE platform.

Product Tested

Symantec Endpoint Protection 11.0.4 MR4 trial in un-managed mode. MR2 in managed mode has also been trialed at customer sites. Symantec Endpoint Protection is supported by Symantec and is not an Avaya product. Please consult Symantec's documentation as required. Versions earlier than MR4 are not authorized for installation on the CallPilot 201i IPE platform.

Installation and Configuration Overview

Use a fully patched and anti-virus protected PC to download the latest AV software, virus definitions, and any needed security patches for Symantec AV security bugs and burn the files onto a CD so that it can be brought to the CallPilot server without using the network. (It is dangerous to use the Internet to download the initial virus definitions after a fresh install of Anti-Virus software. An unprotected computer can become infected in the time it takes to download updates.) Latest virus definitions can be downloaded from web page (look for Symantec Endpoint Protection definitions) at:

http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=savce

There is a self-extracting .exe file named something like **20090123-003-v5i32.exe** under Client installations on Windows platforms (32-bit) section. (Note: the Symantec web site is subject to change and is not under Avaya control.)

Instead of a CD, a USB drive can be used if the CallPilot hardware platform has USB ports (202i IPE, 600r and 1005r Rackmount). Another option is to copy the AV software and definition file to the local hard-drive from a network share before disconnecting the network.

For best security, a CallPilot server must never be connected to the Internet unless it has the latest CallPilot OS Security PEPs, all OS hotfixes authorized for CallPilot and has Anti-Virus software installed with the latest virus definitions. Therefore, unless the network is very well-protected, disconnect the CallPilot server from the network by unplugging both ELAN and CLAN cables before installing the anti-virus software. Be sure you remember where the cables should be plugged back in. (Alternatively, the network interfaces can be temporarily disabled using the control panel.)

Uninstall any existing anti-virus software. Problems will occur if more than one anti-virus product is installed at a time. Reboot if required. (Note, the install of Symantec EndPoint Protection 11 will correctly handle upgrading from a previous version of Symantec Anti-Virus – in this case it is not necessary to explicitly uninstall the previous version.)

Before installing anti-virus software, install all applicable CallPilot OS Security PEPs. Install any additional, authorized hotfixes from CD. (Refer to the latest revision of the CallPilot Server Security Update bulletin).

Be sure that all LAN networking parameters have been fully configured according to site guidelines. In particular, for LiveUpdate to successfully download definitions over the Internet, DNS settings must be properly configured.

If installed according to the instructions given here, antivirus software should have no noticeable impact on CallPilot performance and capacity for normal messaging-related operations. Certain exceptional operations that involve updating a large number of files may operate significantly slower on some platform types due to the added cost of virus scanning. Examples are: software upgrades, PEP installs, restore from backup. You may want to temporarily disable File System Auto-Protect while performing those operations.

Be sure to contact Symantec support to ensure that you have all available software patches for your Symantec Endpoint Protection 11 product.

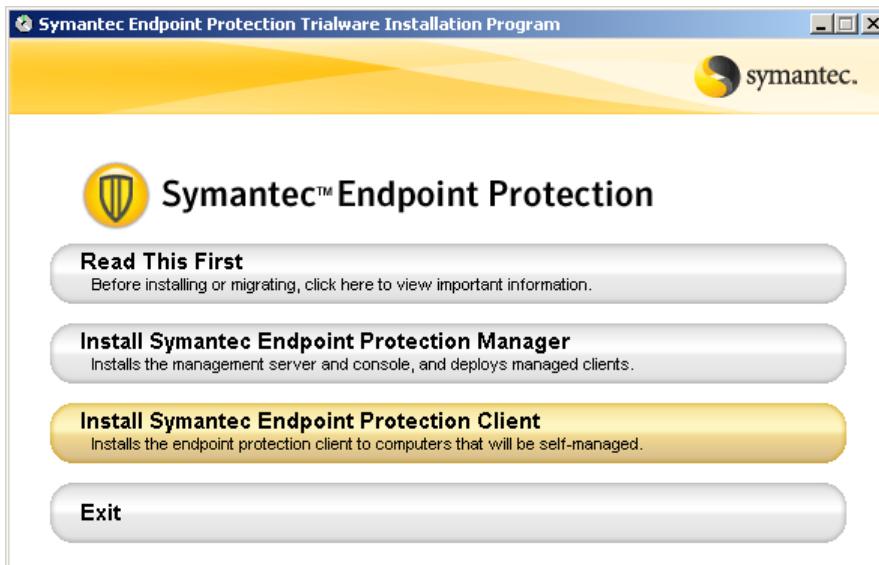
MR4: Space needed when installed on D drive:

Space needed on C drive: 406572 KB

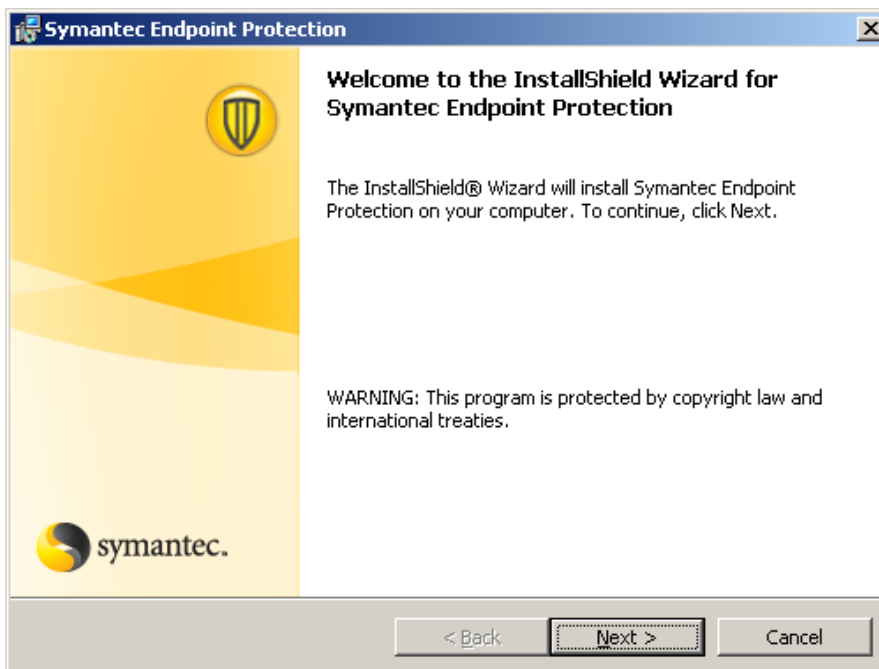
Space needed on D drive: 134644 KB

Installation Instructions

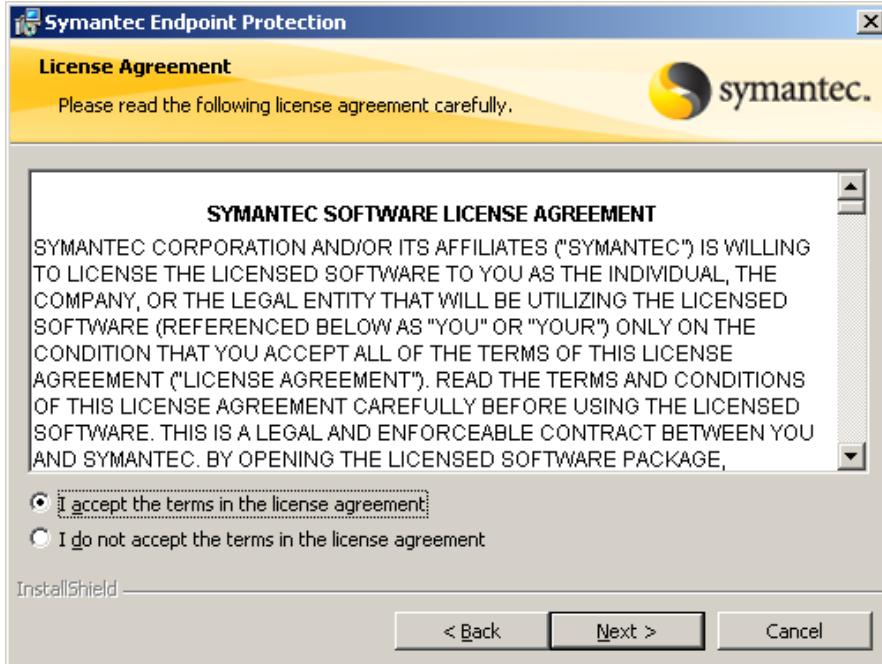
1. Run **Setup.exe**



2. Click **"Install Symantec Endpoint Protection Client"**. **NOTE:** Symantec Endpoint Protection Manager must never be installed on a CallPilot server.



3. Click **"Next"**



4. Read EULA and accept. Then click **“Next”**

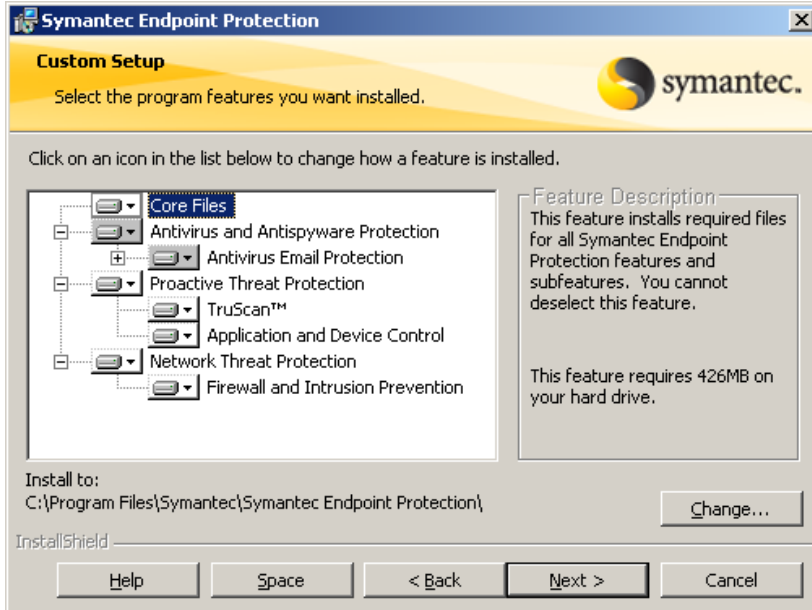


5. Select “Unmanaged client” and click **“Next”**. NOTE: it is acceptable to use a managed client instead, as long as the configuration imposed on the CallPilot server matches the settings described in this document. Managed clients can be configured using Symantec Endpoint Manager. You will probably need to define a “group” within Symantec Endpoint Manager to allow CallPilot servers to have the specific settings they need – those settings are likely to differ from the settings you want to specify for other computers on your network such as desktop PCs.

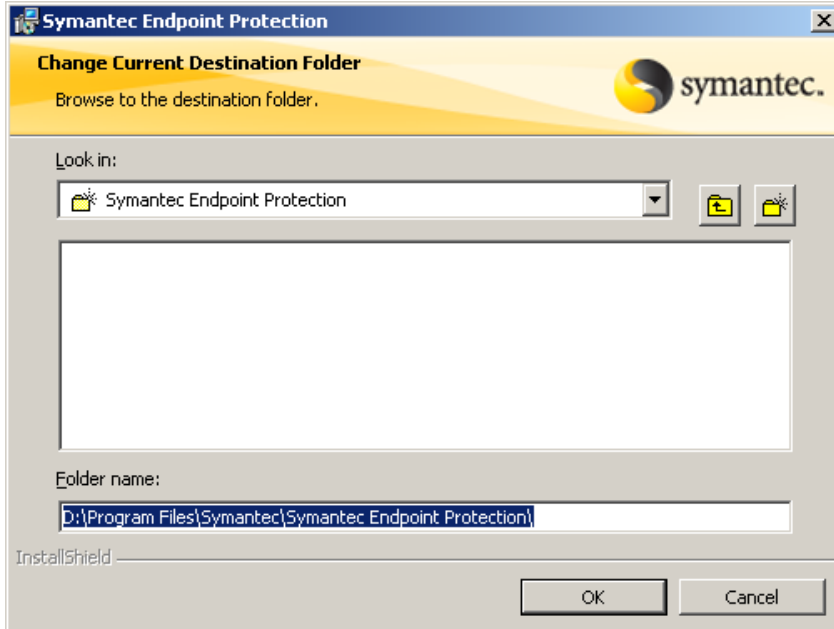
Consult the Symantec documentation. **NOTE:** the Symantec Endpoint Manager and database must never be installed on a CallPilot server.



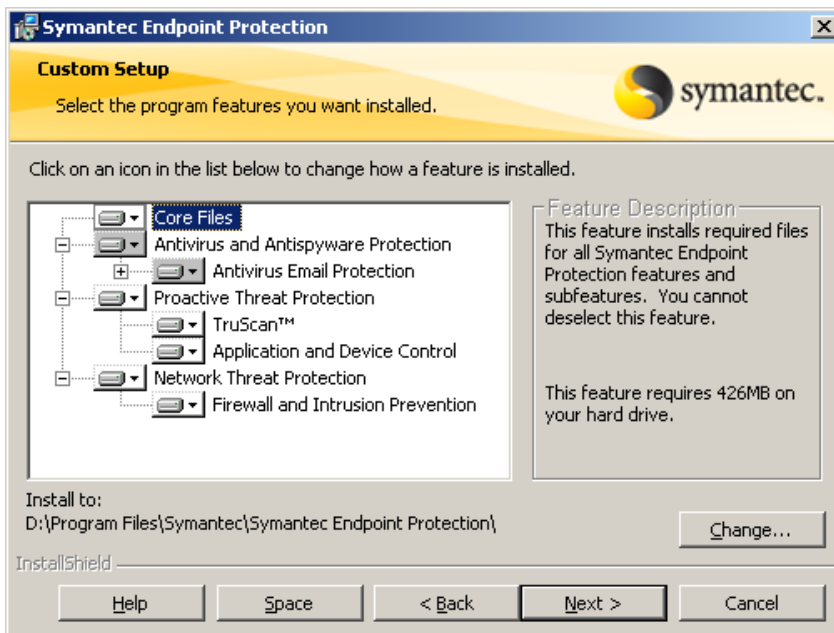
6. Select “Custom” and click “Next”



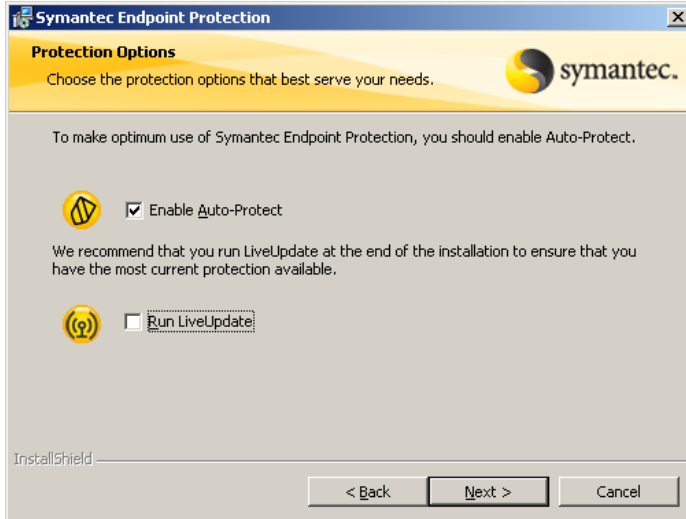
7. For CP3 and CP 4 CallPilot servers, click “Change” and change the C drive to D drive. For CP5, install on the C drive -- you can just click “Next” and skip to step 10



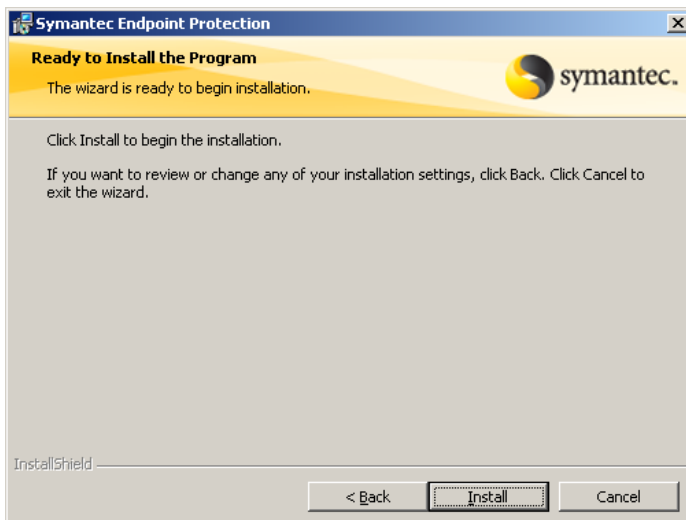
8. Click “OK”



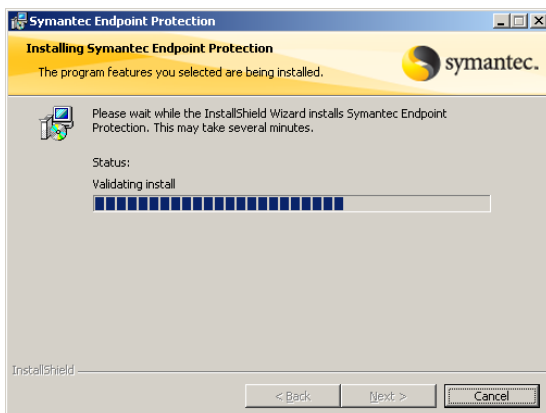
9. **NOTE:** The “Network Threat Protection” feature has been tested and is authorized for use on CallPilot servers. However, it is optional and it is acceptable for a customer to choose to not install this feature. (Some screenshots will change if it is not installed). The “Proactive Threat Protection” feature is not implemented on Windows Server 2003 systems; therefore it does not provide additional protection. A customer may also choose to not install this feature. Click “Next”.

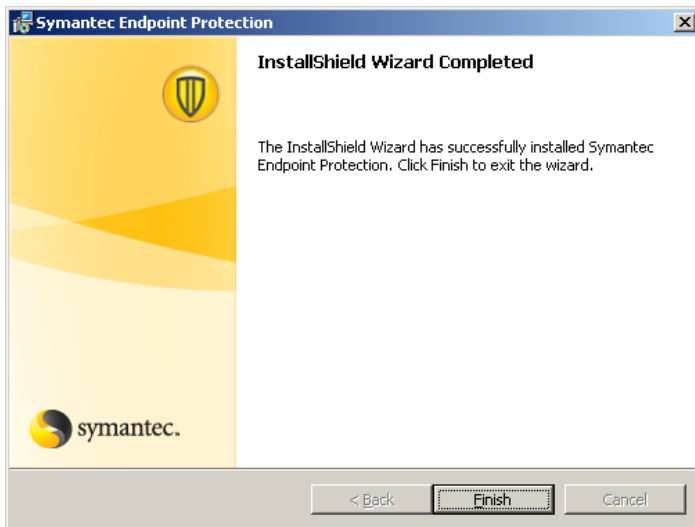


10. Uncheck “**Run LiveUpdate**” (since the network is disconnected), and Click “**Next**”

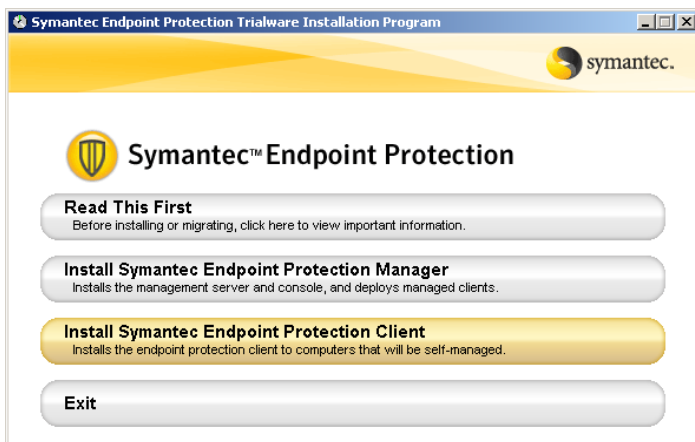


11. Click “**Install**”



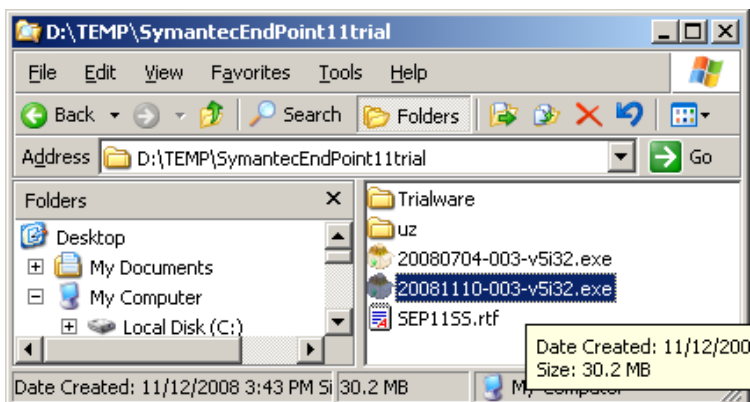


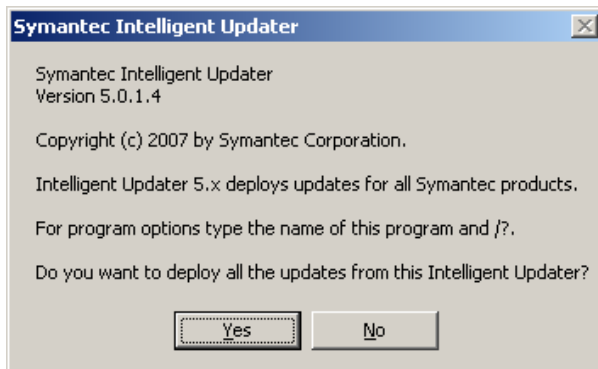
12. Click **"Finish"**



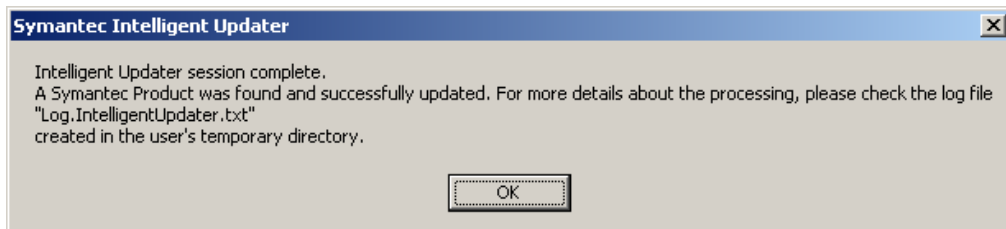
13. Click **"Exit"**. (If it asks you to restart here, please perform the restart, and then log back in).

14. Update definitions using previously downloaded file. Double-click the file once and wait.





15. Click **"Yes"**. Wait ... several minutes with no progress displayed!

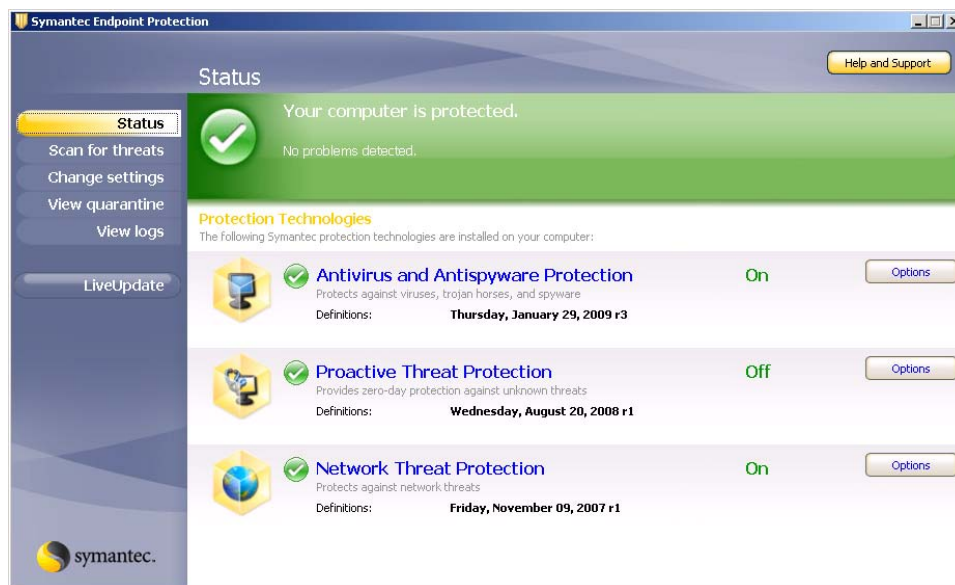


16. Click **"OK"**

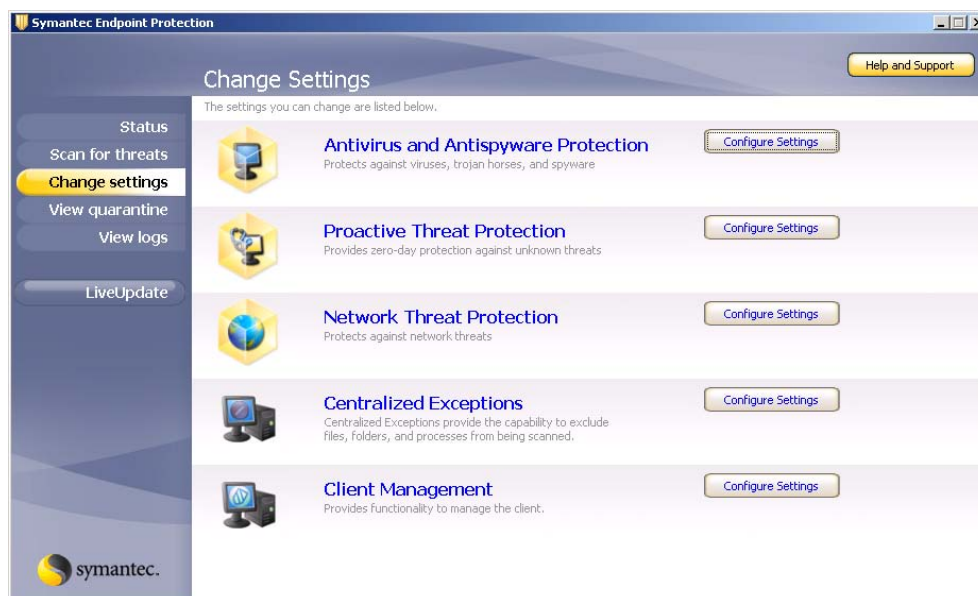
Configuration Instructions

Ensure the display resolution is set to at least 1024x768 for best results.

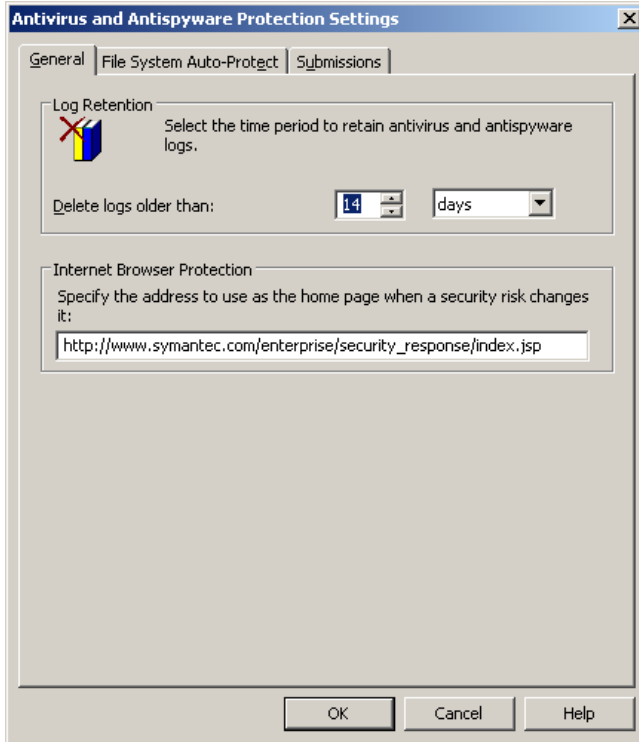
1. Start - Program - Symantec Endpoint Protection - Symantec Endpoint Protection



2. Click "Change settings"

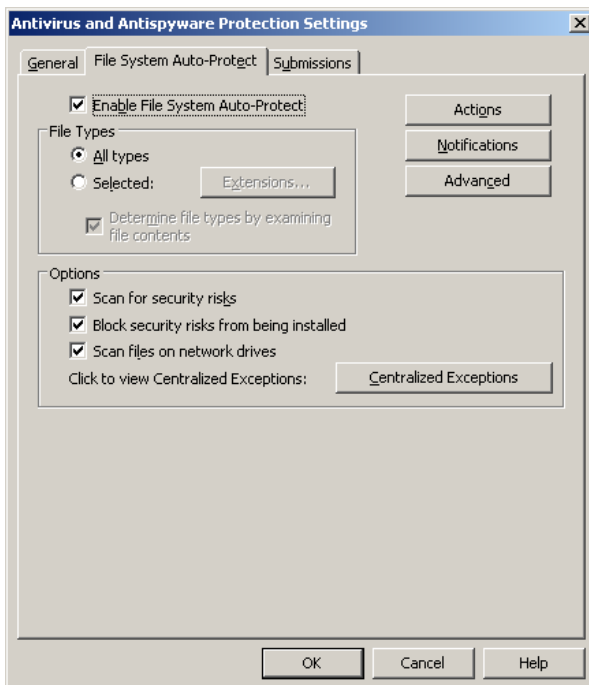


3. Beside "Antivirus and Antispyware Protection", click "Configure Settings"

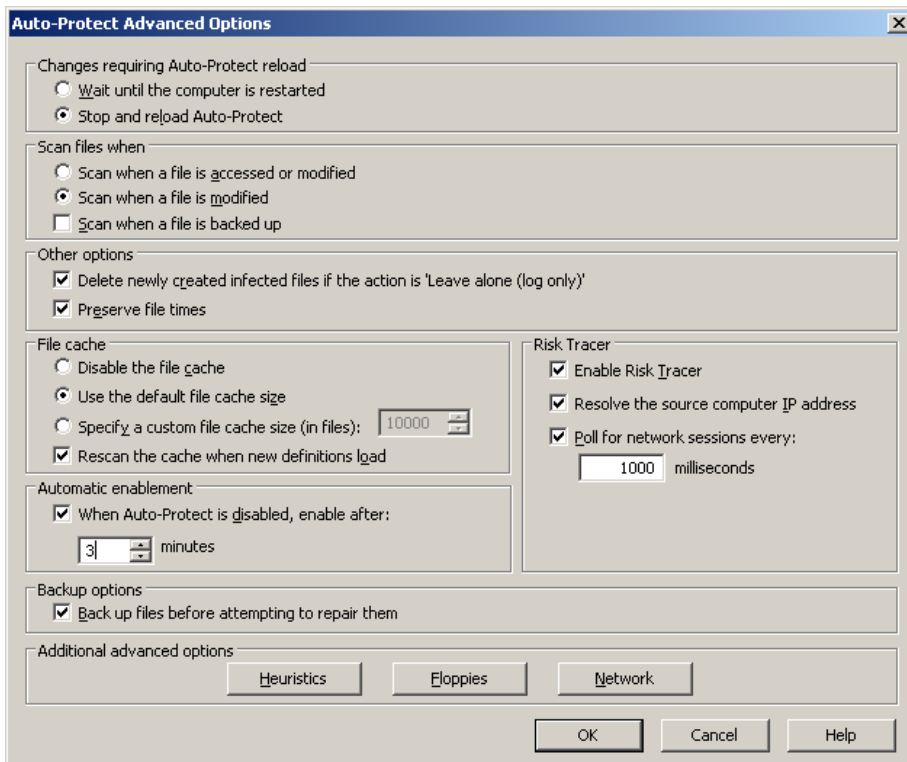


(Under "Internet Browser Protection", customer may wish to change home page URL)

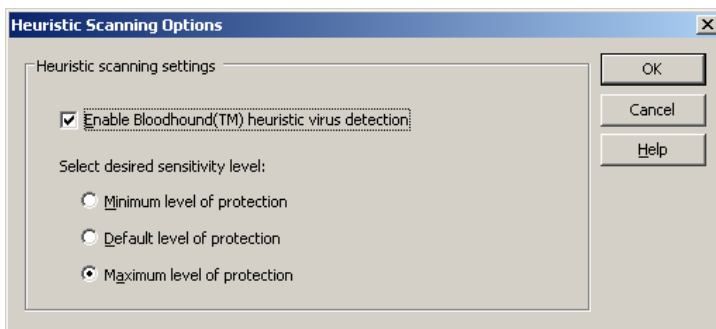
4. Select "File System Auto-Protect" tab



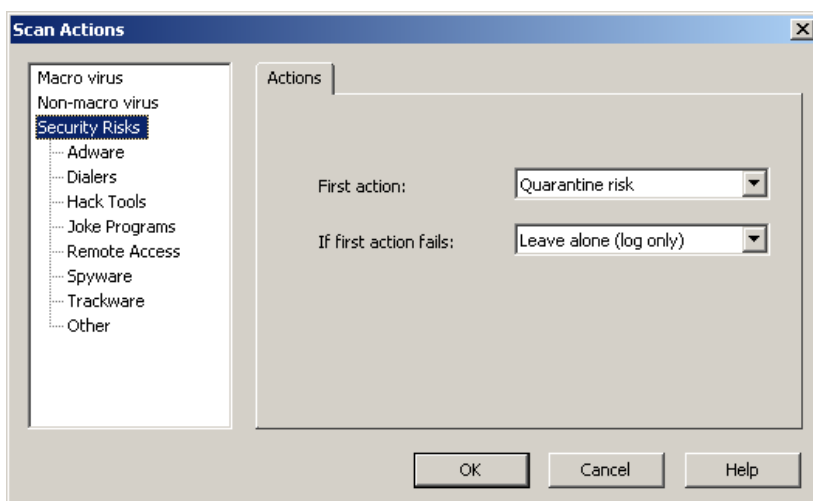
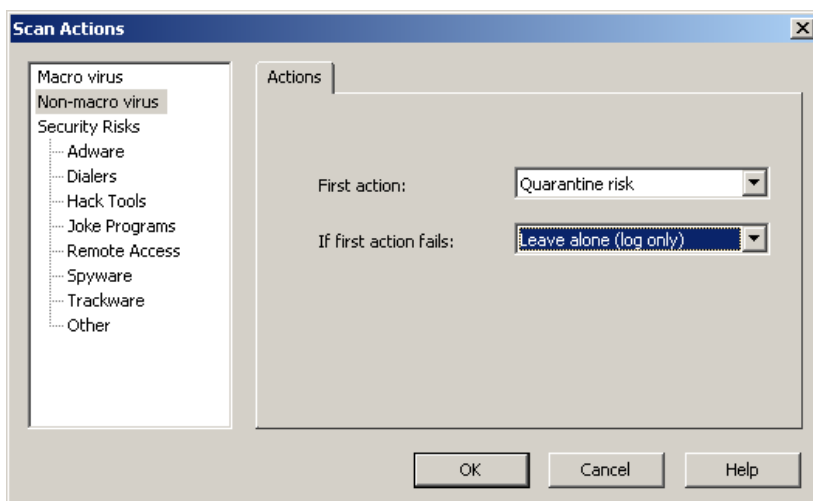
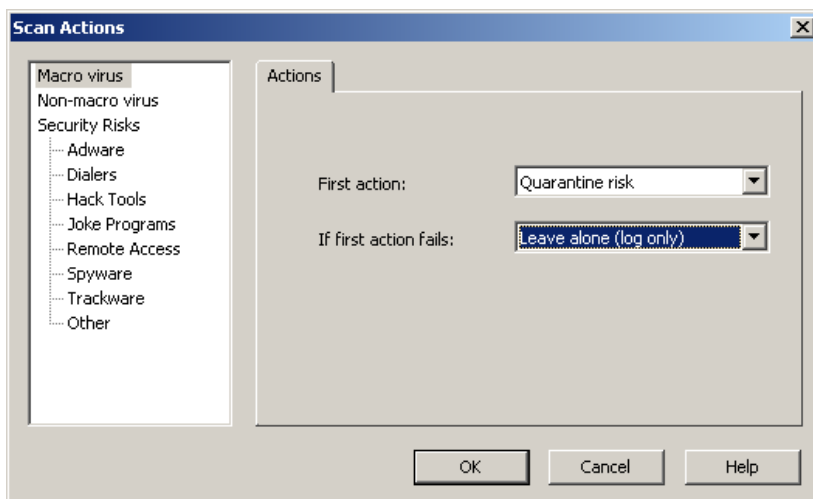
- Click **"Advanced"**. Select **"Scan when a file is modified"**, uncheck **"Scan when a file is backed up"**, and under **"Automatic enablement"** set **"enable after"** to **3** minutes.

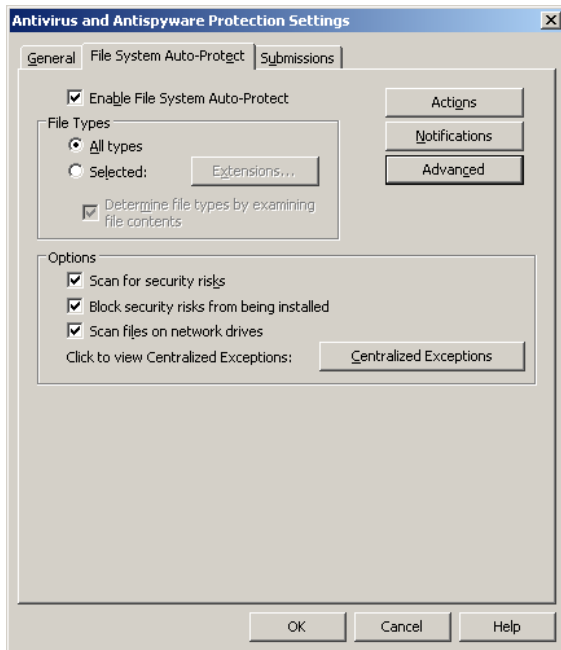


- Click **"Heuristics"**. Select **"Maximum level of protection"**

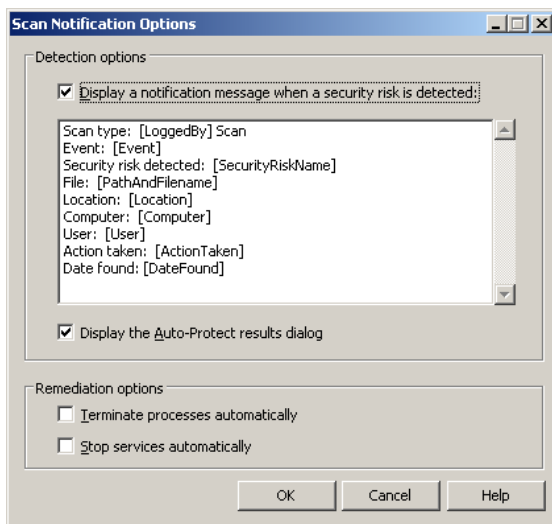


- Click **OK** and again click **OK**
- Click **"Actions"** button. For macro virus, set the first action to "Quarantine risk" and the second action to "Leave alone (log only)". Repeat for non-macro virus and Security Risks. Then click **OK**.

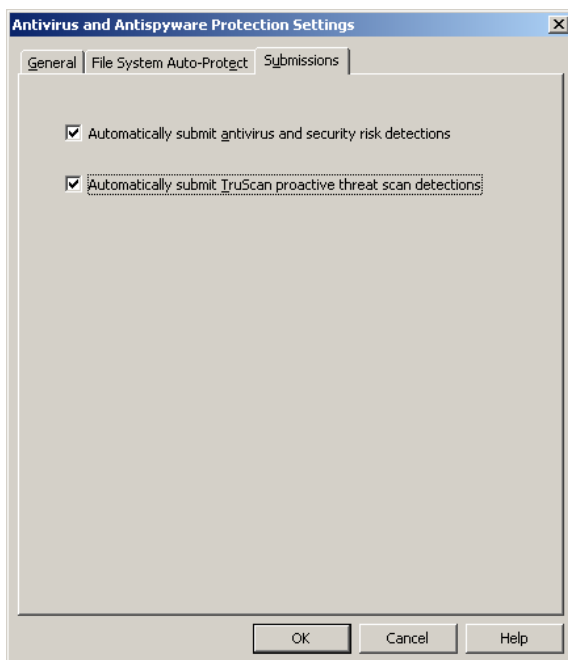




9. Click **"Notifications"**, check **"Display a notification message when a security risk is detected"**



10. Click **"OK"**, then select the **"Submissions"** tab

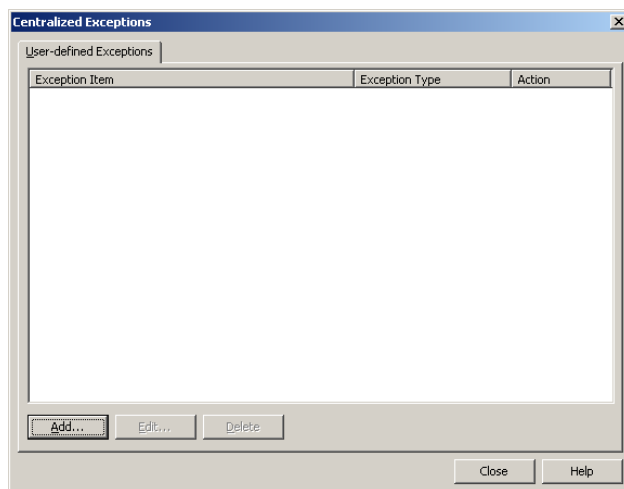


11. Customer may choose to uncheck these two (2) boxes. Click **"OK"**



Note: "Proactive Threat Protection" is not implemented for Windows Server 2003

12. Beside **"Centralized Exceptions"** click **"Configure Settings"**

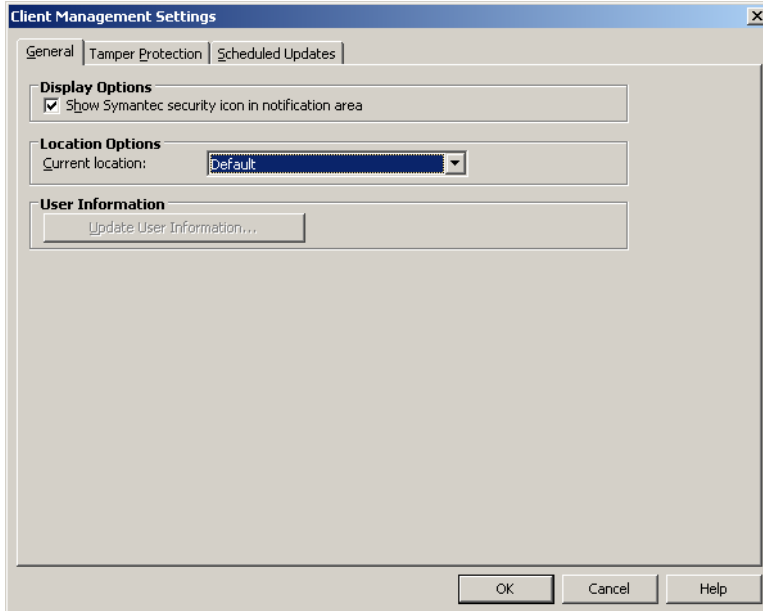


Can add exceptions for "Security Risk Exceptions" or "TruScan Proactive Threat Scan Exception"

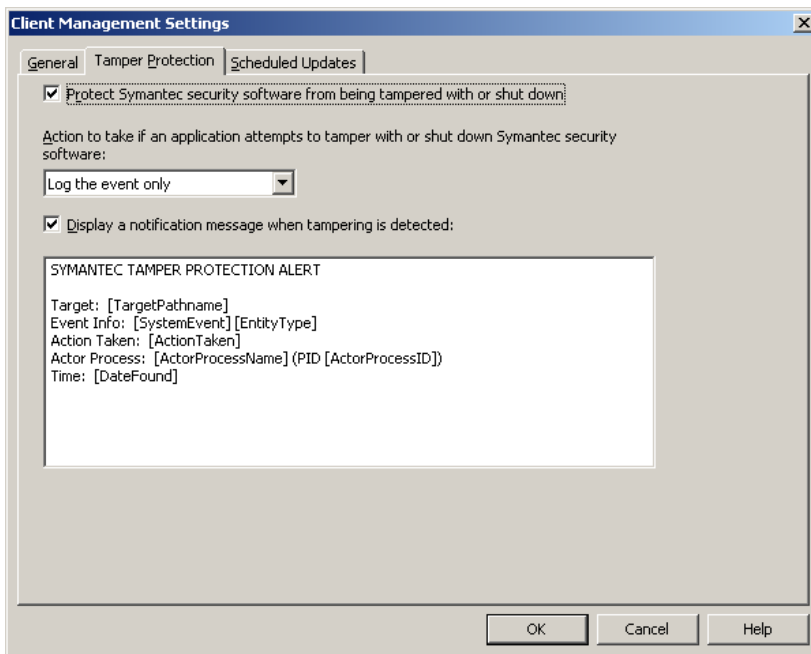
13. It is not necessary to define any exceptions except on a CallPilot "High Availability" configuration. On an HA system, exclude the folder D:\Program Files\EMC AutoStart\<Domain Name>_<Computer Name>. Click **"Close"**



14. Beside **"Client Management"**, click **"Configure Settings"**

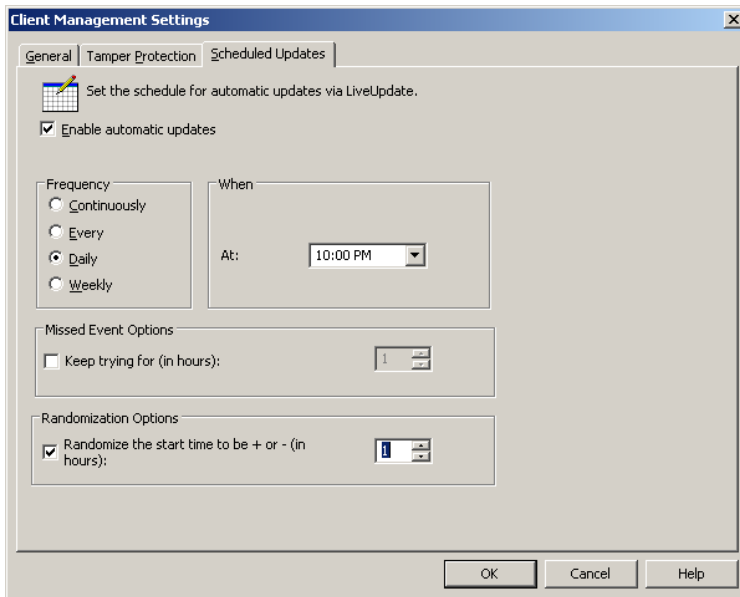


15. Select the "**Tamper Protection**" tab

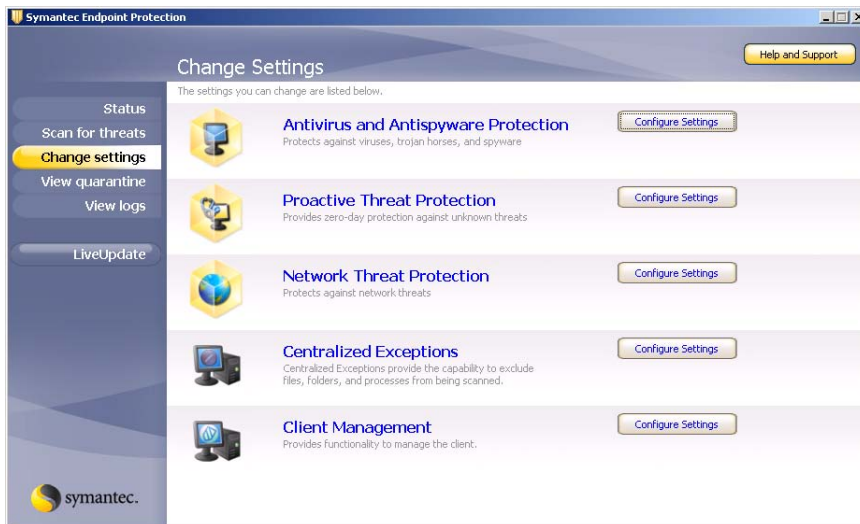


16. Select the "**Scheduled Updates**" tab. Select a time when system load will be light. Optionally uncheck "**Randomize**", or at least set the "Randomization" time to be such that the system load will still be light throughout the randomized interval. **NOTE:** the definition update process will increase CPU and memory usage for about 12 minutes. This can negatively impact CallPilot system performance if performed during a period when the system load is not very low. The simplest approach is to configure updates to occur once a day after the normal office workday is over. In a managed configuration, unless the customer is also running a LiveUpdate server, definitions will typically be pushed out to the entire network at once. Typically the customer's network will include many desktop PCs – since these may be turned off at night, the customer

must push definition updates out during the day. Avaya's testing has not shown any problematic performance impact when definition updates are performed during the day, therefore this is acceptable if necessary.



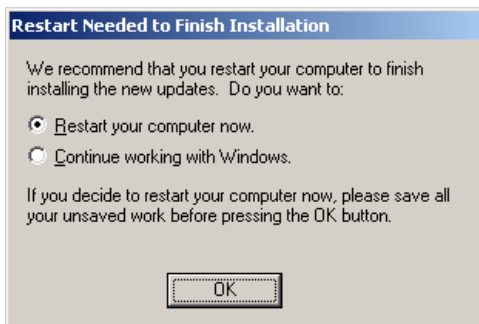
17. Click "OK"



18. Connect network. Then click "LiveUpdate" to get the latest product updates and definitions and to test that the update server can be reached.

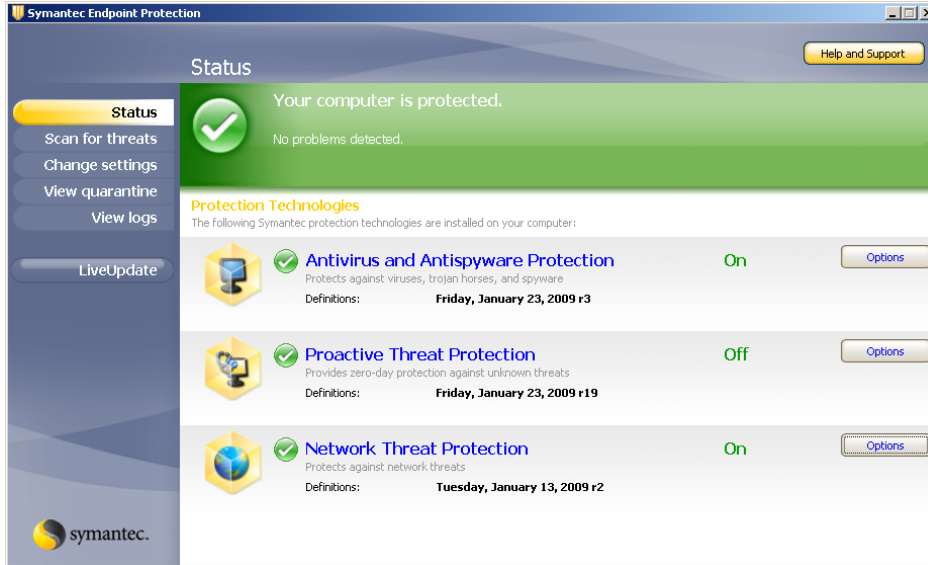


Note: LiveUpdate may download an update for pcAnywhere in addition to Symantec Endpoint Protection. This is not a problem.



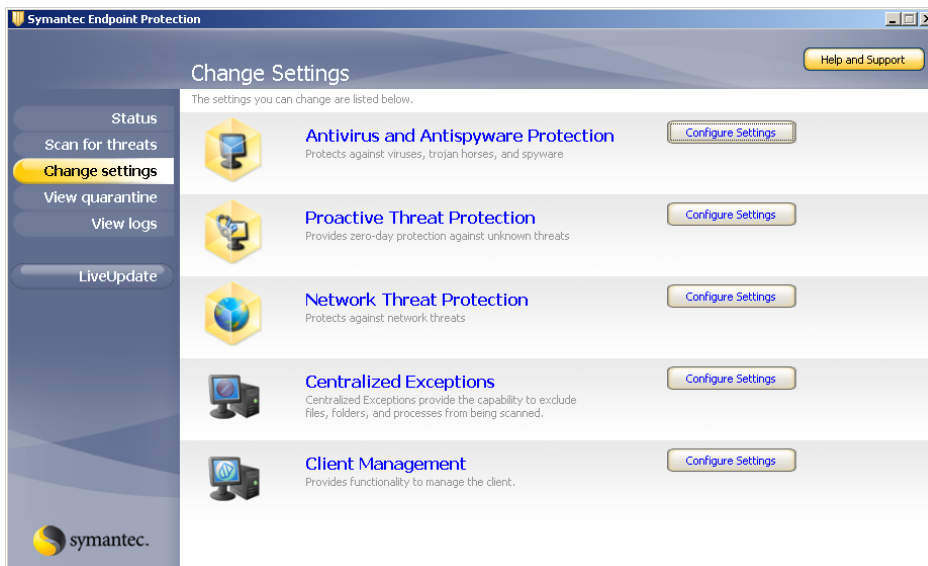
19. Save work and click “**OK**” to restart. After reboot, log back in and wait until system comes back into service.

20. Start - Programs - Symantec Endpoint Protection - Symantec Endpoint Protection

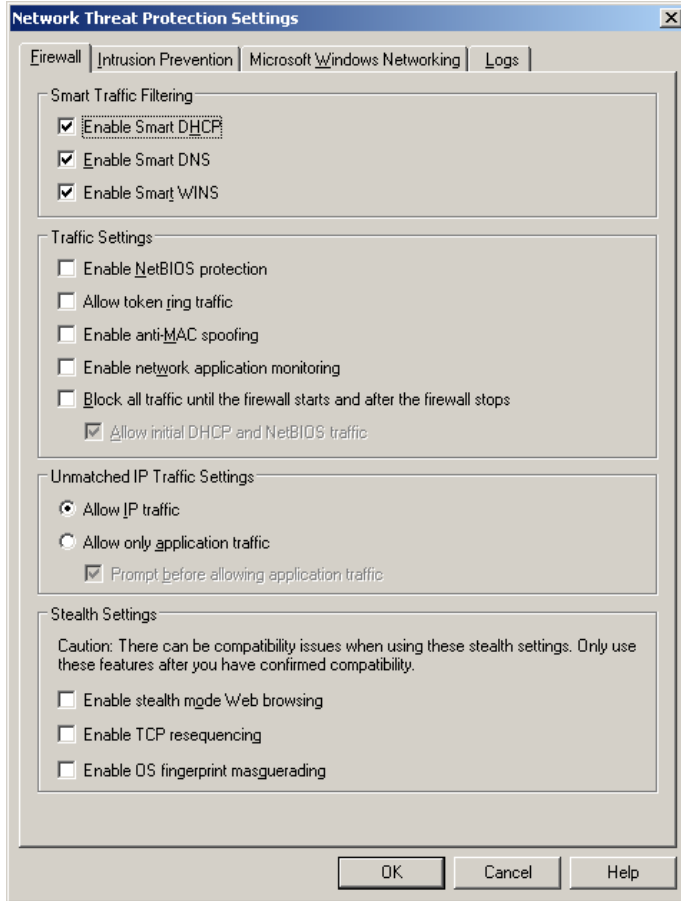


NOTE: "Proactive Threat Protection" does not function on Windows Server 2003.

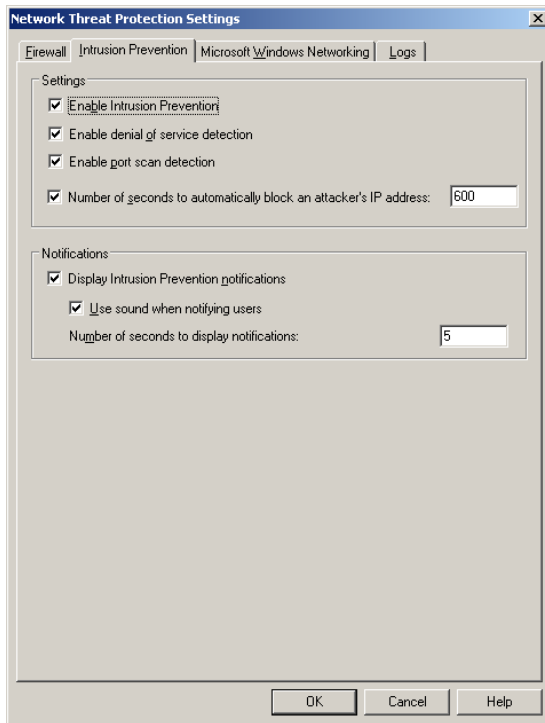
21. Click **"Change settings"**



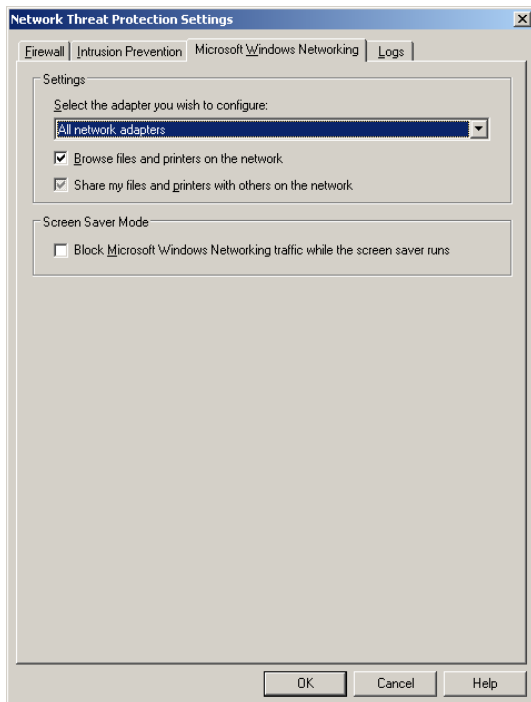
22. Beside **"Network Threat Protection"** click **"Configure Settings"** (Not necessary if this optional feature was not installed).



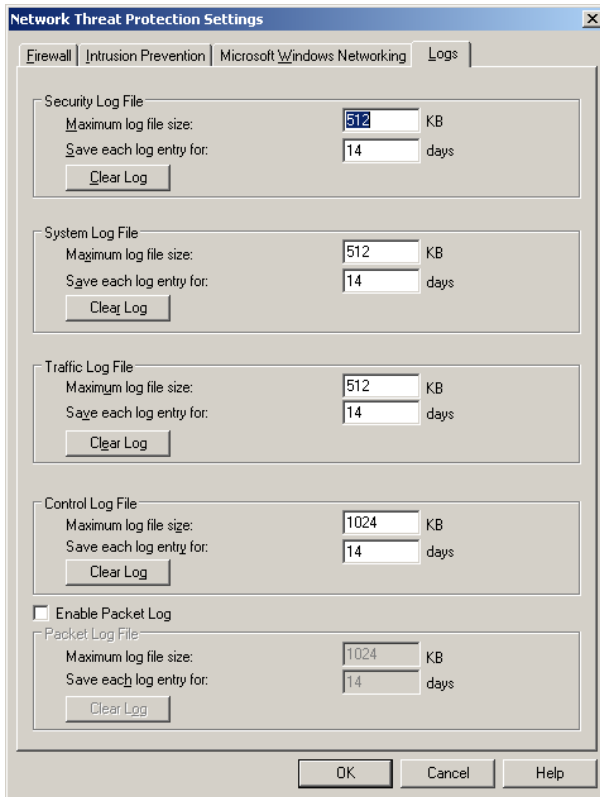
23. Select the "Intrusion Prevention" tab.



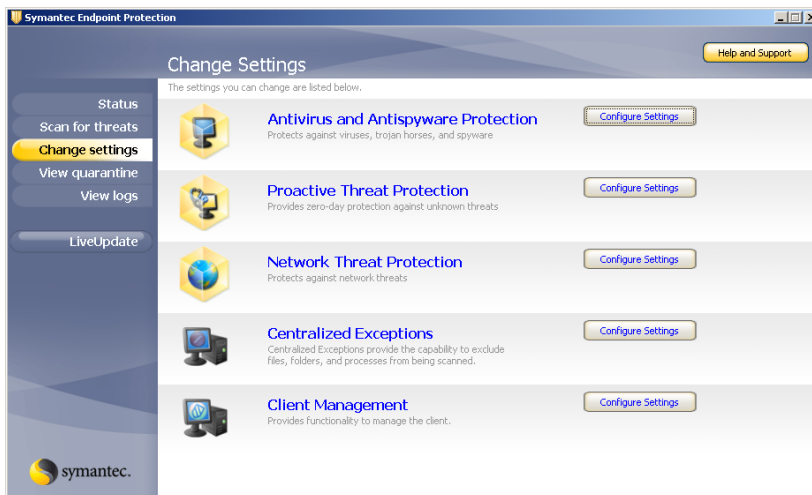
24. Select the "Microsoft Windows Networking" tab



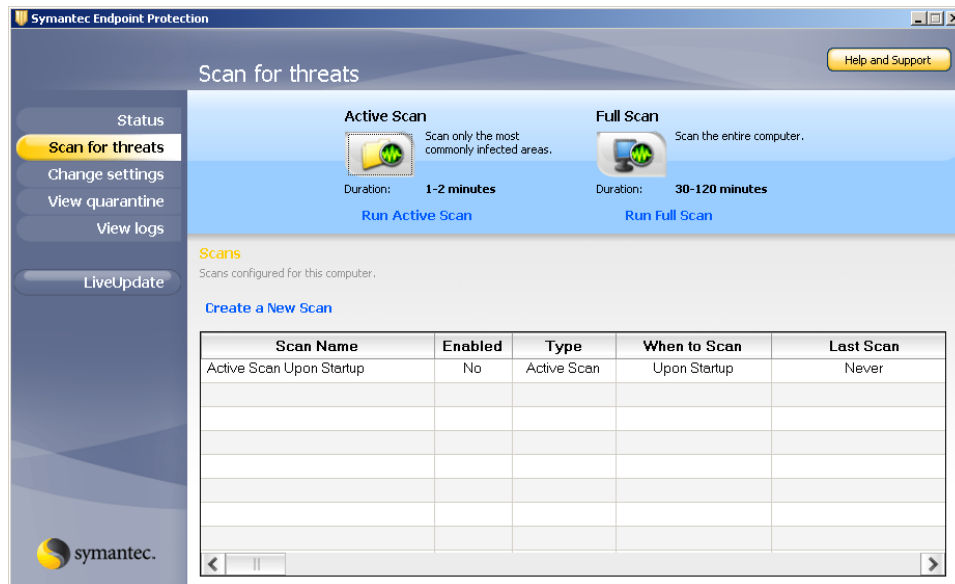
25. Select the "Logs" tab



26. Click "OK"

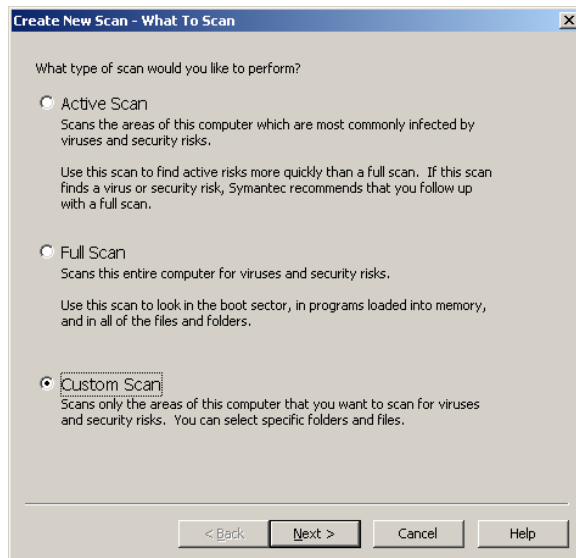


27. Click **"Scan for threats"** in order to set up regular scheduled anti-virus scans

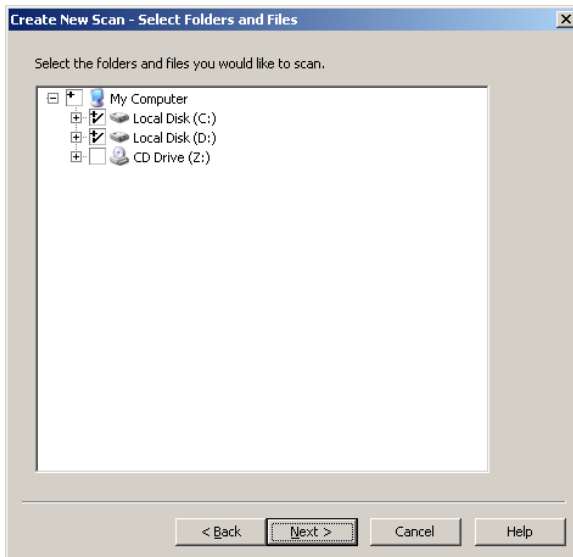


An active scan takes about 8 minutes on 201i. You may want to set up an "Active Scan" every day (at off-hours) and a "Full Scan" every week (at off-hours)

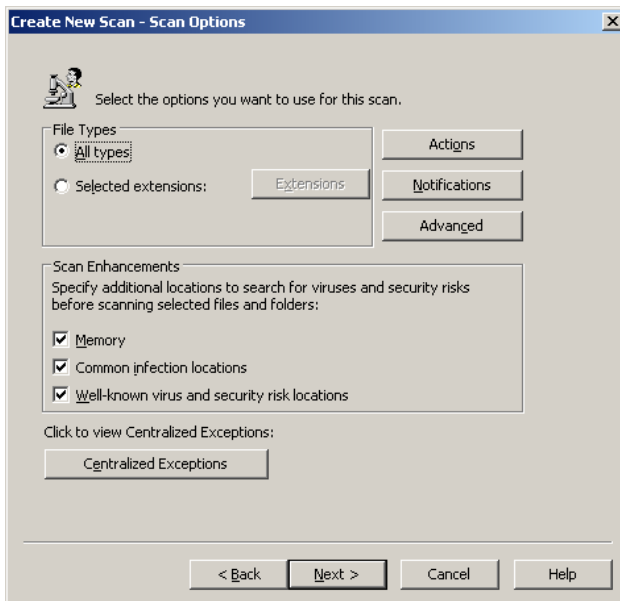
28. Click **"Create a New Scan"**. Select **"Custom Scan"**



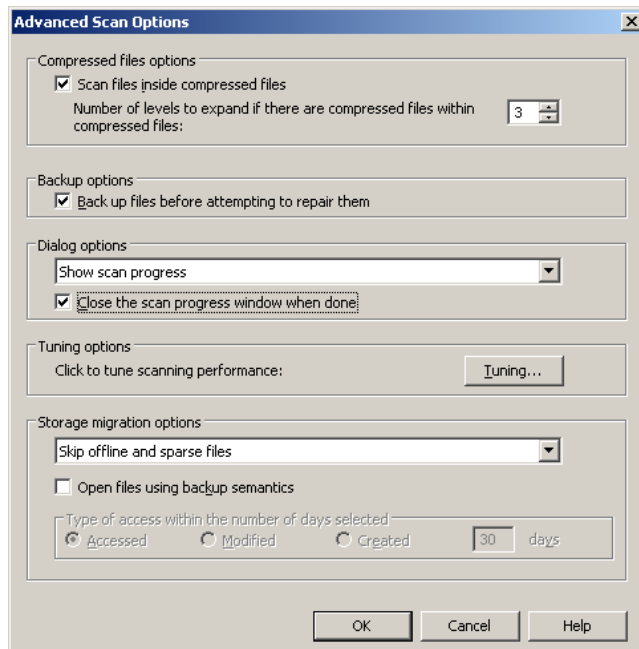
29. Click "**Next**". Select each "**Local Disk**" hard drive. Do not select CD drive or floppy (since problems might occur if a medium read error occurred)



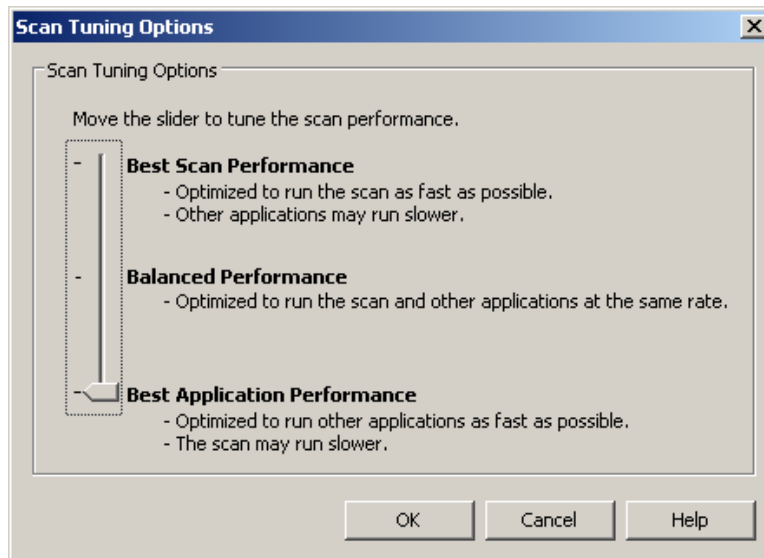
30. Click "**Next**"



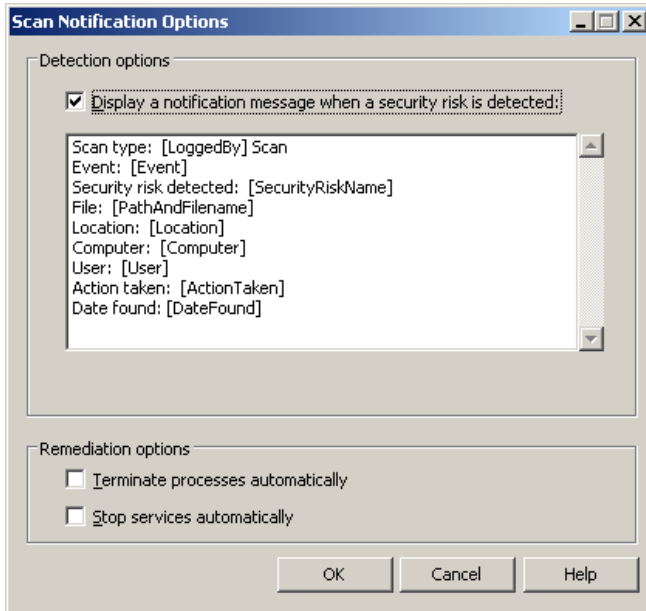
31. Click "**Advanced**". Check "**Close the scan progress window when done**".



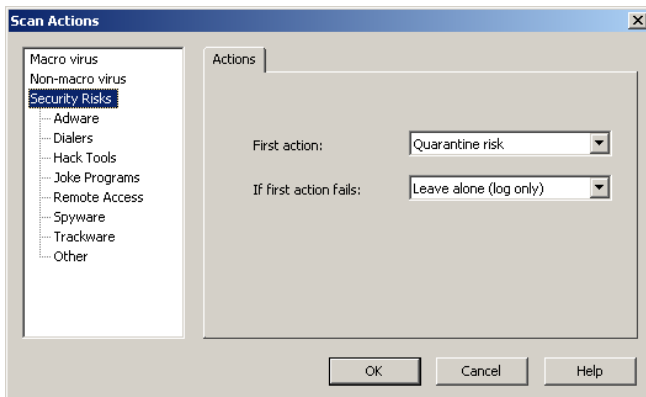
32. Click "**Tuning**". Ensure the slider selects "**Best Application Performance**". Click **OK**.



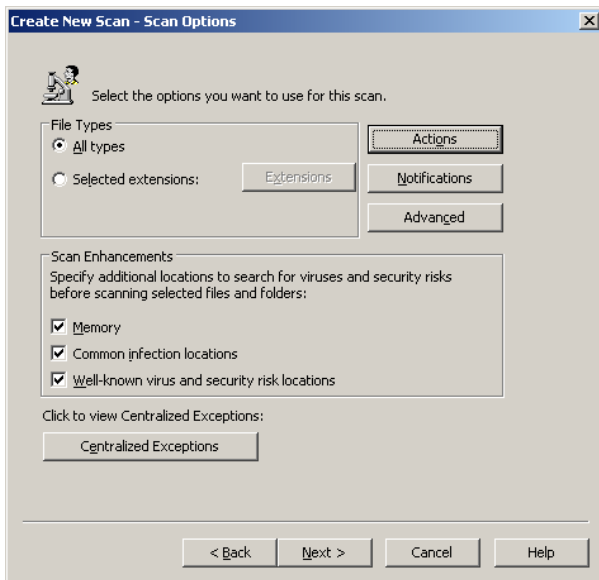
33. Click "OK". Click "Notifications". Check "Display a notification message when a security risk is detected".



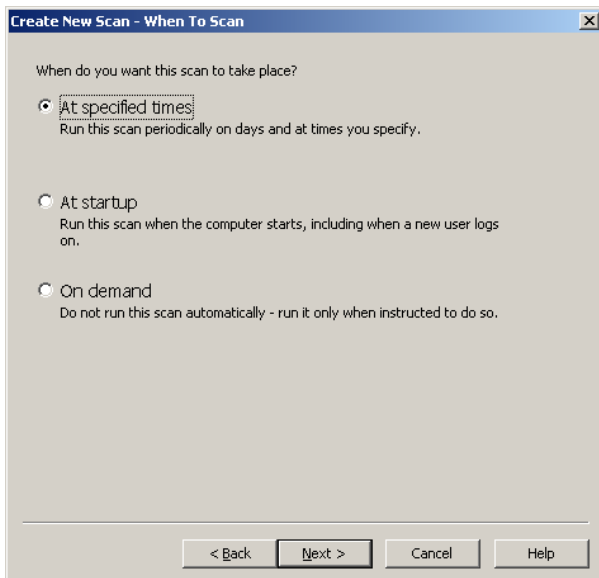
34. Click "OK". Click "Actions". Ensure Action for "Security Risks" has first action set to "Quarantine risk". Occasionally anti-virus products can have "false positives" that, for a given definition file, might mark a valid CallPilot or Windows file as a virus. By using the quarantine setting, it will be possible to restore the file if this happens.



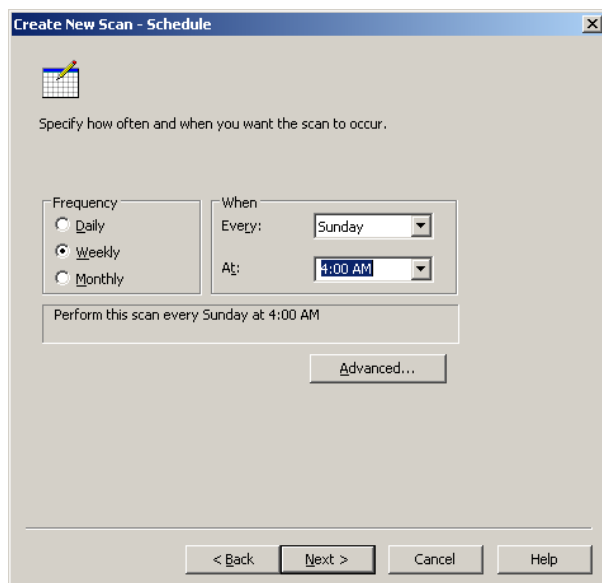
35. Click "OK"



36. Click "Next"



37. Ensure "At specified times" is checked, click "Next". Select an appropriate time for the scan. Ensure that the CallPilot system load is expected to be very low for the entire period of time when the scan will run. A full scan on a 201i platform takes about 4 ½ hours. (It may take less time on other CallPilot platforms). The scan duration does not depend to any great extent on the number of messages stored on the server.



Create New Scan - Schedule

Specify how often and when you want the scan to occur.

Frequency:

- ☐ Daily
- ☒ Weekly
- ☐ Monthly

When:

Every: Sunday

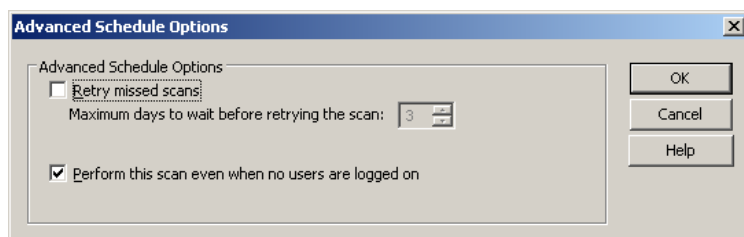
At: 4:00 AM

Perform this scan every Sunday at 4:00 AM

Advanced...

< Back Next > Cancel Help

38. Click "**Advanced...**". Uncheck "**Retry missed scans**". This is important to ensure that a scan will not get started at an inappropriate time.



Advanced Schedule Options

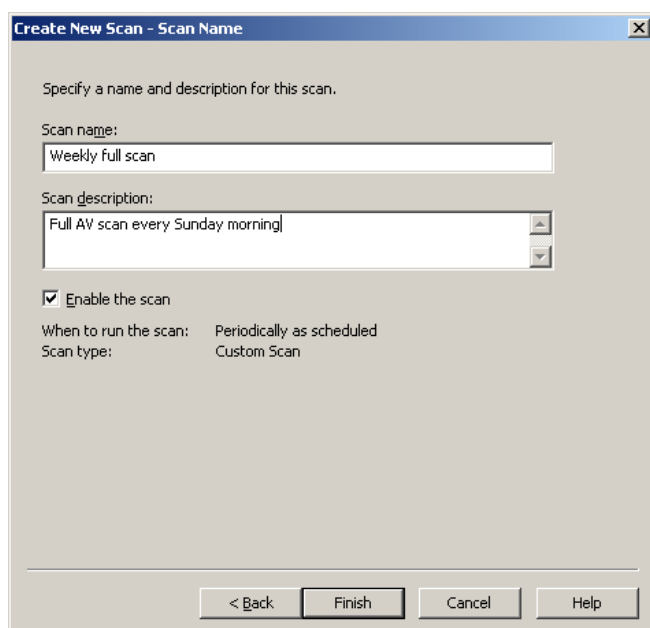
Advanced Schedule Options

☐ **Retry missed scans**
Maximum days to wait before retrying the scan: 3

☒ **Perform this scan even when no users are logged on**

OK
Cancel
Help

39. Click "**OK**" then click "**Next**"



Create New Scan - Scan Name

Specify a name and description for this scan.

Scan name:
Weekly full scan

Scan description:
Full AV scan every Sunday morning

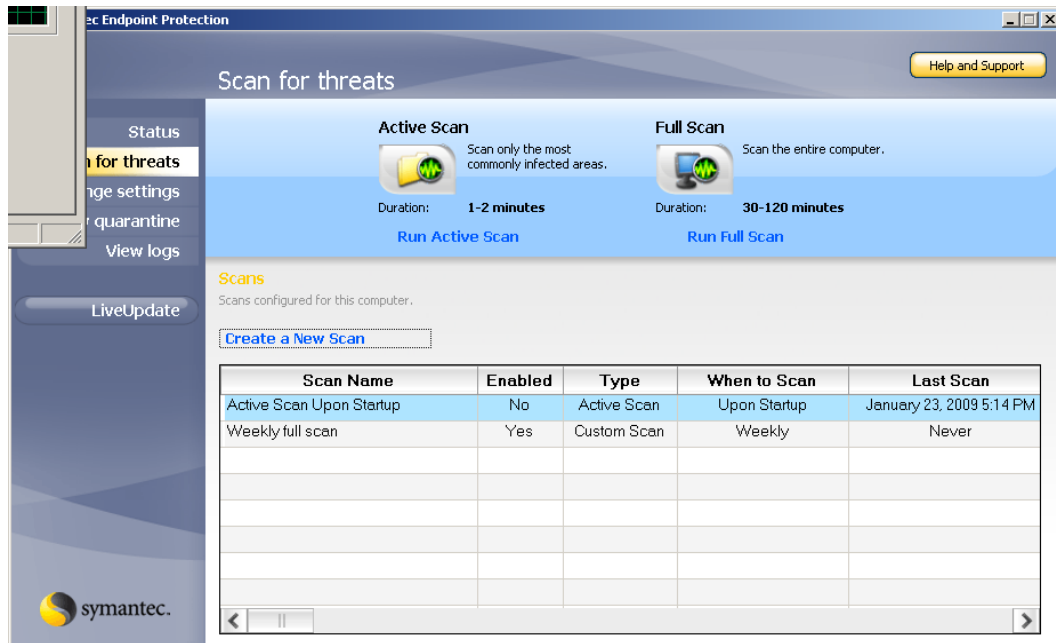
☒ **Enable the scan**

When to run the scan: Periodically as scheduled

Scan type: Custom Scan

< Back Finish Cancel Help

40. Specify a name for the scan and type a description, then click "**Finish**"

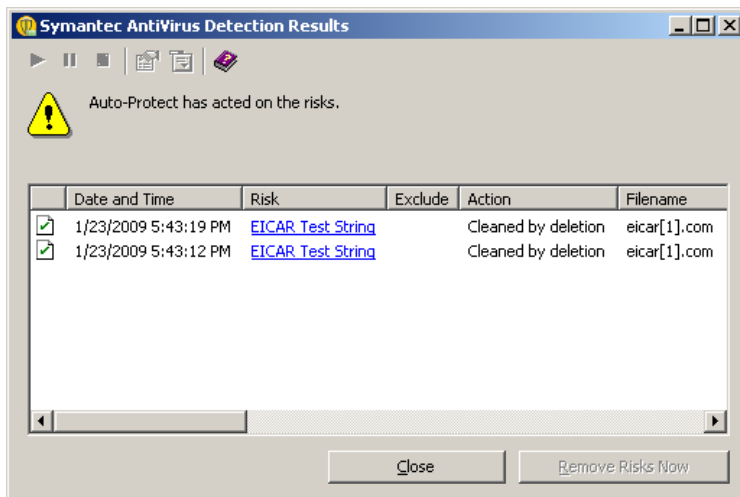
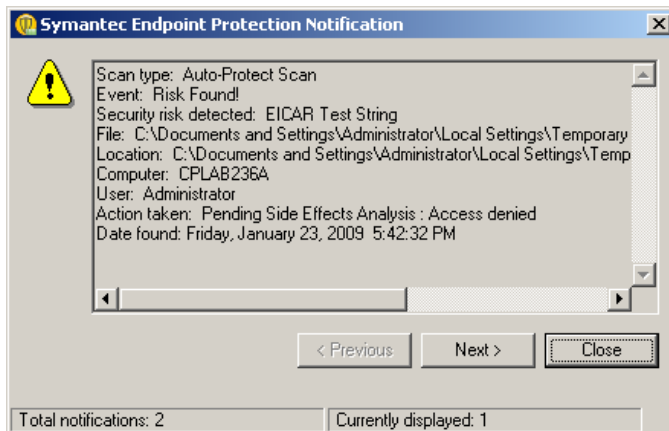


NOTE: Full scan on 201i takes about 4.5 hours.

41. Close "**Symantec Antivirus Protection**" window

Test

Go to <http://www.eicar.org>. Try downloading the various test files available on the site.



Processes

Here is a list of processes associated with SEP 11 and their memory usage.

Process	Description	Typical Virtual Memory usage during normal CallPilot operation	Maximum Virtual Memory usage observed
Checksum.exe	CMC checksum		
ControlAP.exe			
DoScan.exe			
dot1xtray.exe	802.1x Supplicant		
DWHWizrd.exe			
LUALL			3 MB
LuaWrap.exe	LuaWrap Module		
LUCallBackProxy			3.3 MB
LUComServer			5 MB
nlnhook.exe			
PatchWrap.exe	CMC PatchWrap		
Rtvscan.exe		7.8 MB	63 MB
RtvStart.exe			
SavUI.exe			
SescLU.exe	Endpoint Security Client Live Update		3 MB
Smc.exe	CMC Smc (firewall?)	5 MB	16.5 MB
SmcGui.exe	CMC SmcGUI	2 MB	6.9 MB
smcinst.exe	Client Management Component		
SNAC.EXE	Network Access Control		
SymCorpUI.exe	GUI for Symantec Endpoint Protection		15.9 MB
SymDelta.exe	CMC Communication		
WSCSAvNotifier.exe			

Space requirements given by vendor in this screen:

- Core Files: 426 MB
- Antivirus and Antispyware Protection 14 MB (sub-features 2444KB)
- Proactive Threat Protection 1 KB (sub-features 139 MB)
- TruScan 4955 KB
- Application and Device Control 134 MB
- Network Threat Protection 0 KB (sub-features 229KB)
- Firewall and Intrusion Protection 229 KB

Appendix-E

This appendix provides Installation and Configuration procedures for CallPilot 5.0 servers utilizing the **Trend Micro OfficeScan 10.5** anti-virus application.

Product Features

- Powerful network management capabilities
- Can do real-time scanning on file modification only

Product Deficiencies

- Seems to lack “stand-alone” install capability. An anti-virus server must be set up. Installing OfficeScan on a CallPilot server will require the assistance of customer IT personnel who manage the OfficeScan server.
- No apparent way to schedule pattern updates on a per-client basis
- No apparent way to install and update anti-virus server with network disconnected.
- Does not write event logs into Windows event log subsystem
- Some important settings are global and cannot be individually set on a server-by-server basis

Product Tested

Trend Micro OfficeScan 10.5 trial.

Installation and Configuration Overview

OfficeScan 10.5 is inherently a network managed anti-virus solution intended to protect a network of computers. Before you can install OfficeScan 10.5 on a CallPilot server, you first need to install an OfficeScan server (if you do not already have one). You update this server, then use it to create a “Client Installation Package” that you can deliver (on CD or USB drive) to a (possibly disconnected) CallPilot server. Then, management of the OfficeScan parameters is done primarily using the OfficeScan server’s web console. It is possible to allow certain OfficeScan functions to be controlled locally on the client.

These guidelines are not intended to replace the OfficeScan documentation from Trend Micro. Please consult the OfficeScan documentation for more information as required. Note that OfficeScan is not an Avaya product. If you have problems with OfficeScan, please make use of Trend Micro support resources.

Also, please be sure that you have obtained all relevant OfficeScan bug fixes and patches. Consult your Trend Micro representative. Software bugs in anti-virus software can cause serious problems, including system outages and security vulnerabilities.

Installing the OfficeScan server

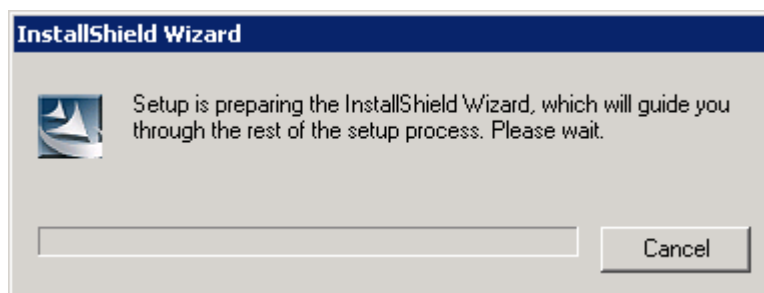
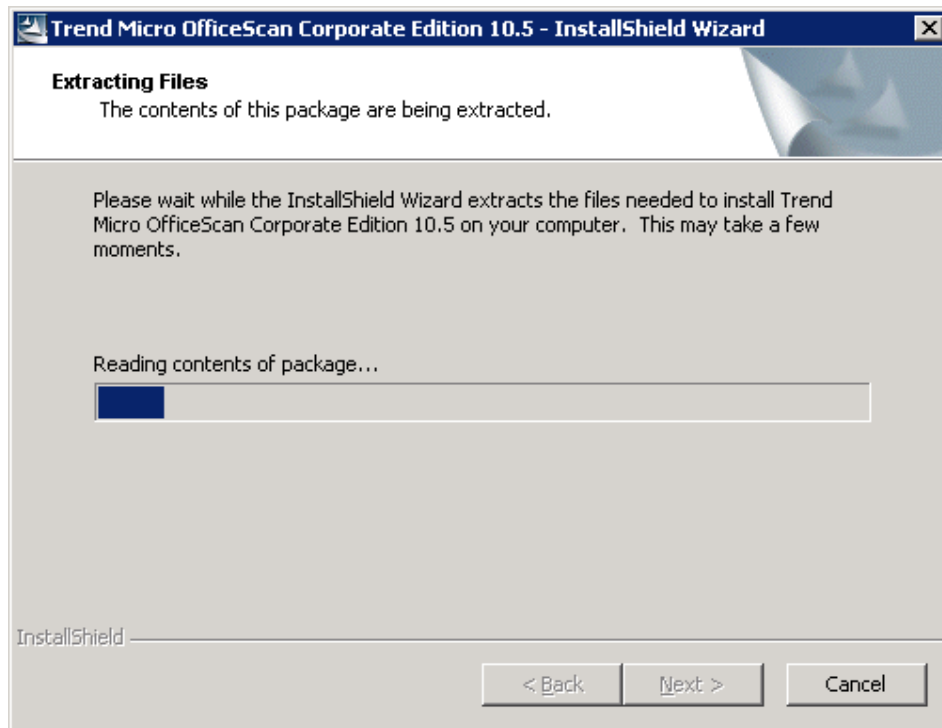
Typically a customer wishing to use OfficeScan to protect a CallPilot server will already have an OfficeScan server set up for managing the rest of their network. If so, skip this section and go to **Preparing an OfficeScan Client Package for CallPilot servers and Installing it**.

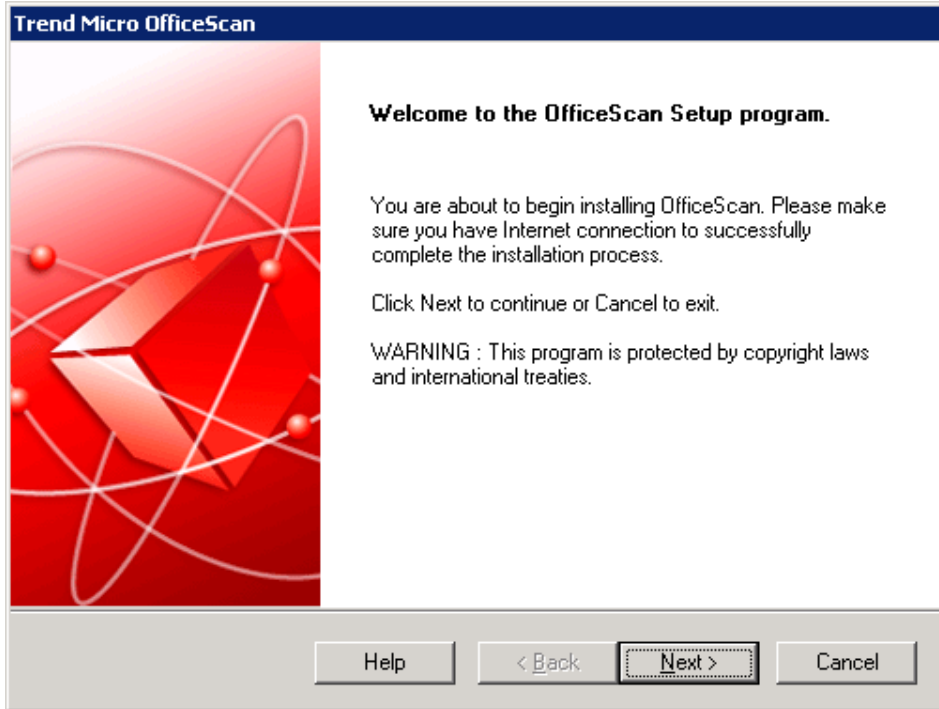
If you need to set up an OfficeScan server (e.g. for a test environment) you will need a separate PC running Windows Server 2003, 2003 R2, 2008, 2008 R2, Windows Storage Server 2003 R2, 2008. (Note: a CallPilot server must never be used as an OfficeScan server since this will consume excessive resources on the CallPilot server and could impact CallPilot performance.) Check the system requirements published by Trend Micro for the OfficeScan server.

The computer to be used for the OfficeScan server needs to have networking fully set up and enabled, including DNS settings.

Note: Avaya strongly recommends using a scheduled maintenance window for the installation since, in some cases, a system reboot may be required.

1. On the OfficeScan 10.5 CD, double-click “**setup.exe**”

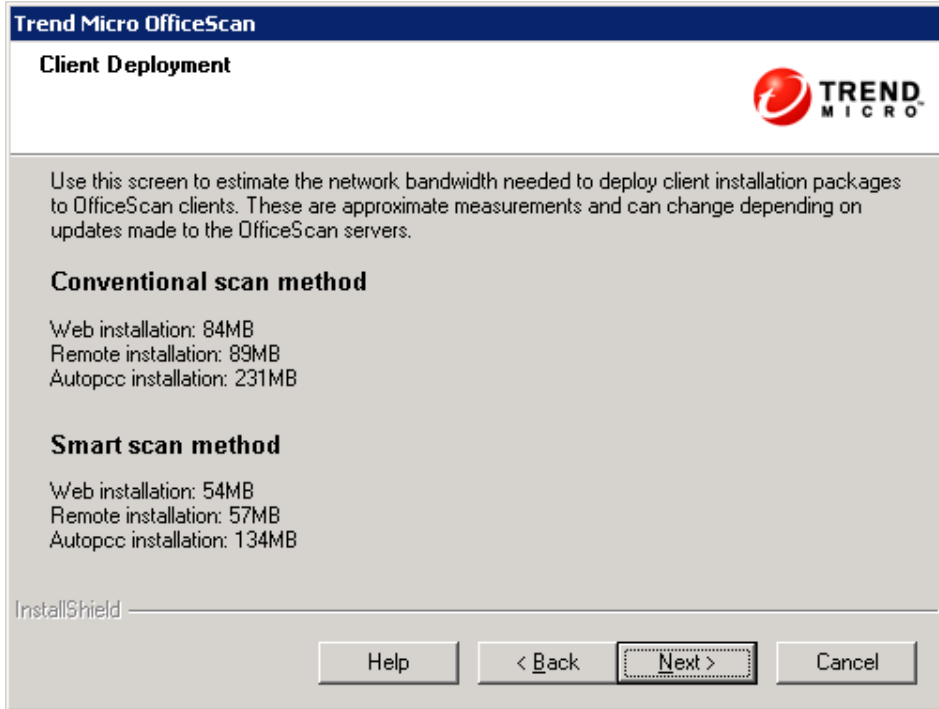




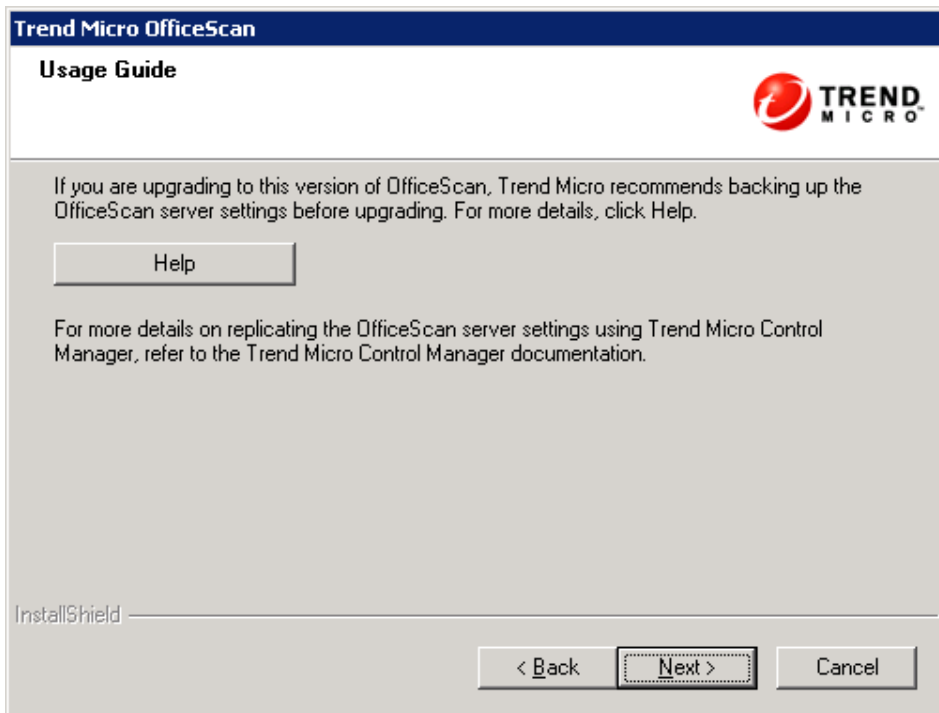
2. Click "Next"



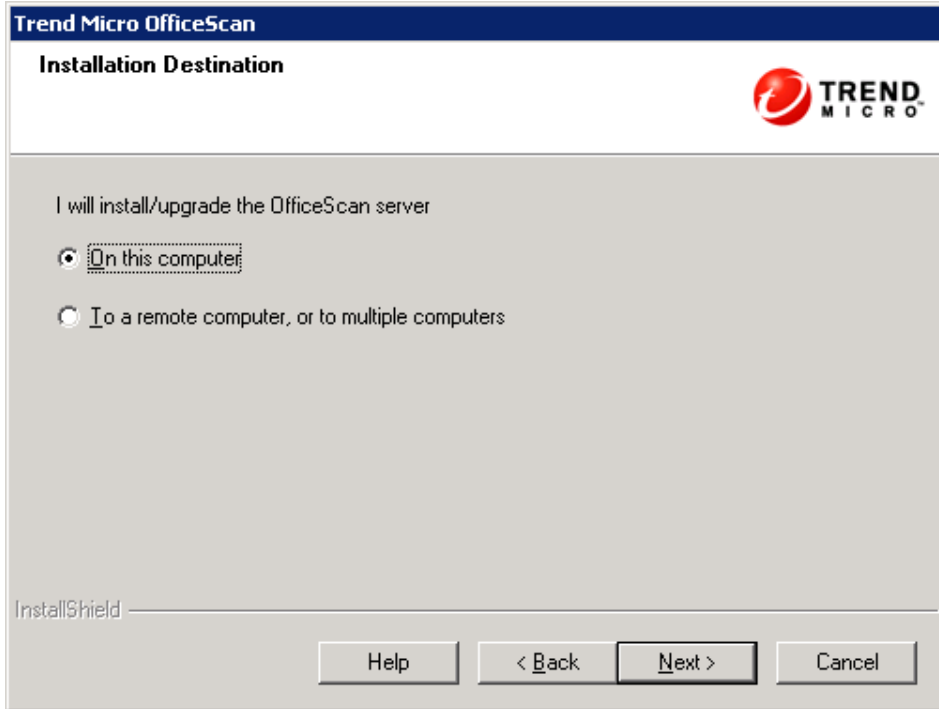
3. Select "I accept the terms..." and click "Next"



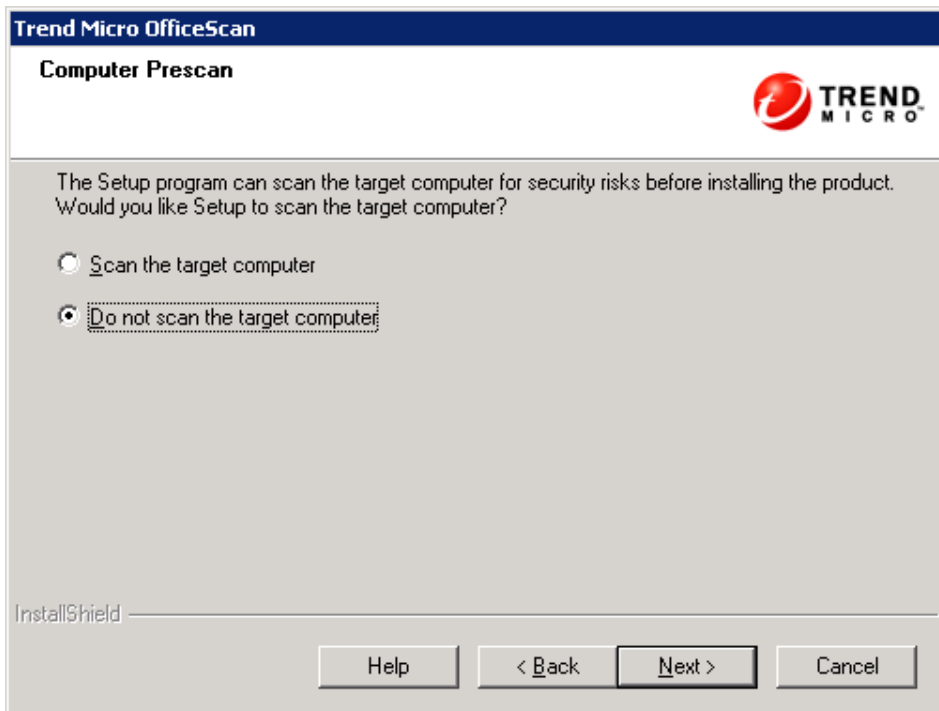
4. Click "Next"



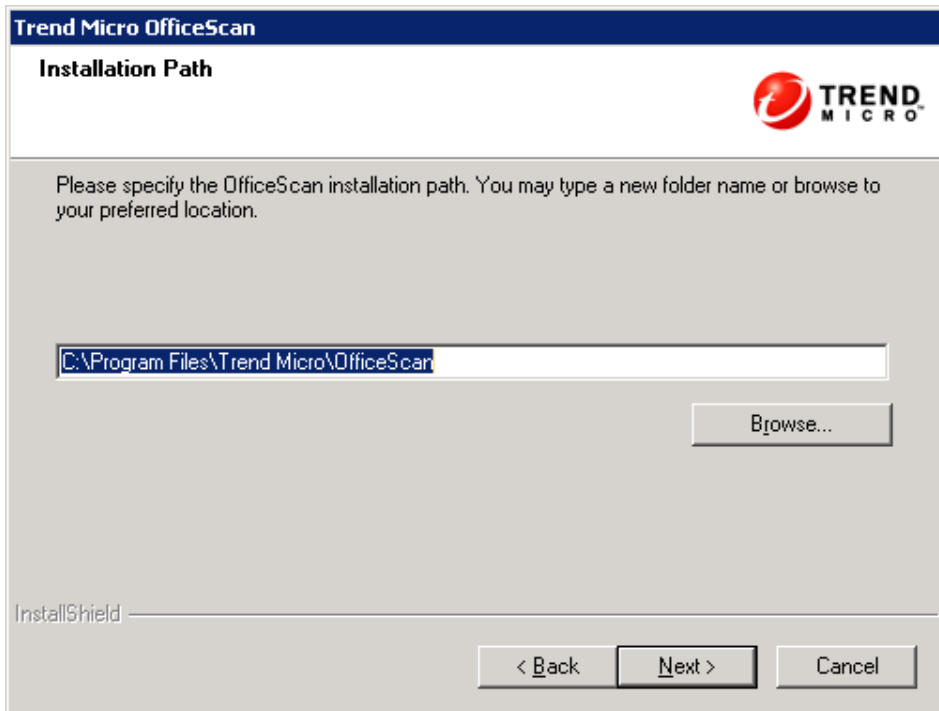
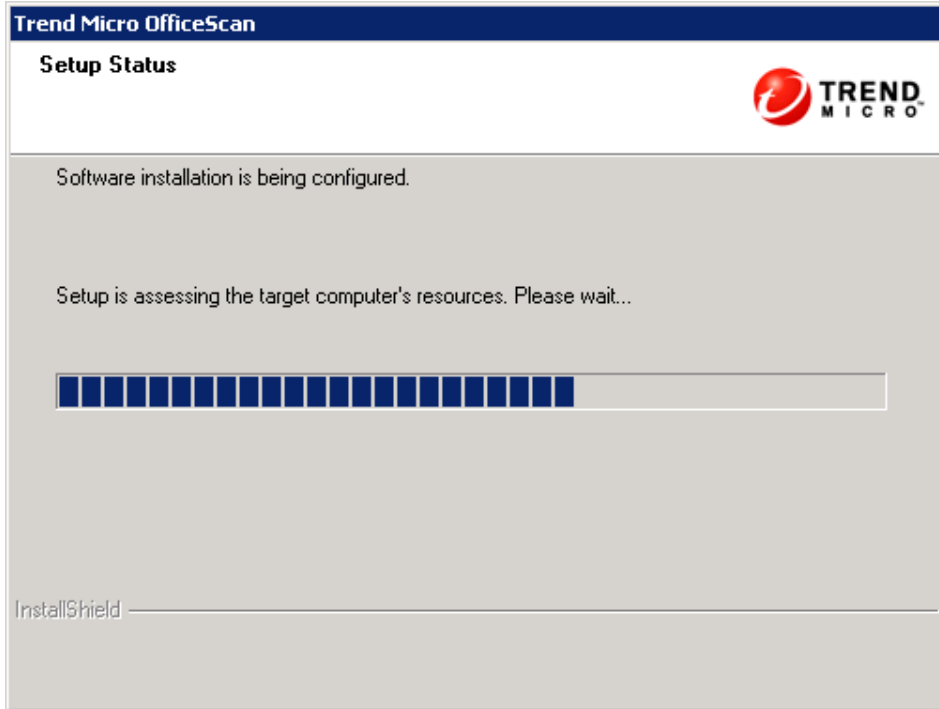
5. Click "Next"



6. Select "On this computer" and click "Next"



7. Select "Do not scan the target computer" and click "Next". (You may choose to scan if you want, however scanning is best done after updating the scan engine and pattern files.)



8. Specify the installation path for the OfficeScan server software or leave it at its default. Click "Next"

Trend Micro OfficeScan

Proxy Server

If you use a proxy server to access the Internet, specify your proxy settings below. OfficeScan will use this information when downloading updates from the Trend Micro update server.

Proxy settings

☐ Use a proxy server

Proxy type: ☒ HTTP ☐ SOCKS 4

Server name or IP address:

Port:

Authentication (optional):

User name:

Password:

InstallShield

Help < Back Next > Cancel

9. If a proxy server is used for the OfficeScan server to access the Internet, configure it. Otherwise, if no proxy server, just click "Next".

Trend Micro OfficeScan

Web Server

Please choose the Web server to use for the OfficeScan server.

☒ IIS server

☐ Apache Web server 2.0 (will be installed if not yet installed)

HTTP port:

☒ Enable SSL

Certificate validity period: year(s)

SSL port:

InstallShield

Help < Back Next > Cancel

10. The OfficeScan server is administered using a browser to access a web console. The OfficeScan server needs a web server to use for this. If your computer already has IIS installed, it can use that. Otherwise, it will install Apache Web server 2.0 as its web server. Choose the appropriate options for the web server, ports and SSL, then click "Next".

Trend Micro OfficeScan

Computer Identification

Specify whether OfficeScan clients will identify the server by its domain name or IP address.

Trend Micro recommends using an IP address when the computer has multiple network cards and using a domain name when the computer's IP address is subject to change.

☒ Domain name: mdsclient1

☐ IP address: 192.168.21.99

InstallShield

Help < Back Next > Cancel

11. Select either domain name or IP address as the means to identify the OfficeScan server. (Typically domain name would be used here). Click "Next"

Trend Micro OfficeScan

Product Activation

Step 1. Register online

Activation is a two-step process:

- 1) Register online (Skip this step if you already have the Activation Code).
- 2) Enter the Activation Code.

Use the Registration Key that came with your product and click the button below to register online. An Activation Code will be sent to you via email.

Register Online

InstallShield

Help < Back Next > Cancel

12. If you already have the activation codes, click "Next". Otherwise you may have to register online.

Trend Micro OfficeScan

Product Activation

Step 2. Enter the Activation Code(s)

Type the Activation Codes for the OfficeScan services using the following format:
(XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX)

Antivirus:

OS [REDACTED] KMSG

Damage Cleanup Services:

OS [REDACTED] KMSG

Web Reputation and Anti-spyware:

OS [REDACTED] KMSG

InstallShield

Help < Back Next > Cancel

13. Fill in the activation codes. Click “Next” (Trial codes expire 1 month from when they were first obtained from Trend)

Trend Micro OfficeScan

Install Integrated Smart Protection Server

By default, setup will install an Integrated Smart Protection Server on the target computer with Smart Scan as the default scan method. This server supports HTTP and HTTPS protocols. Configure settings for this server from the OfficeScan Web console.

To ensure optimal performance, Trend Micro recommends installing the standalone Smart Protection Server.

If you disable the Integrated Smart Protection Server, change the Scan method to Conventional scan from the OfficeScan Web console to ensure continued protection.

Install the integrated server. This server supports HTTP and HTTPS protocols.

☒ Enable SSL

Certificate validity period: 3 year(s)

SSL port: 4345

InstallShield

Help < Back Next > Cancel

14. Click “Next”

Trend Micro OfficeScan

Enable Web Reputation Service

Setup will enable an integrated Web Reputation Service on the target computer.

Do you want to enable the integrated Web Reputation Service?

☐ No

☒ Yes. Enable the integrated Web Reputation Service.

HTTP port:

InstallShield

Help < Back Next > Cancel

15. You can enable Web Reputation Service on the target computer. Make your selection and click “Next”.

Trend Micro OfficeScan

Install Other OfficeScan Programs

Aside from the OfficeScan server, you may want to install other OfficeScan programs to the target computer. Select from the programs below:

☒ OfficeScan client (can be installed only if ServerProtect for NT is not installed on the target computer)

☐ Policy Server for Cisco NAC

☐ Cisco Trust Agent for Cisco NAC

Type the full path of the local drive and directory where the Cisco Trust Agent certificate file is located (for example: c:\ctagent.cer).

The certificate must be located on a local drive; mapped drives are not acceptable.

Import Certificate...

InstallShield

Help < Back Next > Cancel

16. In addition to installing the OfficeScan server software, you probably want to also install the OfficeScan client software onto the AV server machine so that computer can be protected from viruses. If so, check the OfficeScan client box. Click “Next”.

Trend Micro OfficeScan

Smart Protection Network





The Trend Micro Smart Protection Network is a next-generation cloud-client content security infrastructure designed to deliver proactive protection against the latest threats.

☐ **Enable Trend Micro Smart Feedback (recommended)**

When enabled, Smart Feedback shares anonymous threat information to the Smart Protection Network for analysis. You can disable Smart Feedback anytime through the product console.

Your industry (optional): Not Specified

InstallShield

Help
< Back
Next >
Cancel

17. Optionally, you can enable Trend Micro Smart Feedback. Make your selection and click “Next”.

Trend Micro OfficeScan

Administrator Account Password



Specify the passwords for opening the Web console or unloading/uninstalling the OfficeScan client. Passwords prevent unauthorized modification of Web console settings or removal of the OfficeScan client.

Web console password:

Account: root

Password: xxxxxx

Confirm password: xxxxxx

Client unload and uninstall password:

Password: xxxxxx

Confirm password: xxxxxx

InstallShield

Help
< Back
Next >
Cancel

18. Specify a password for logging into the OfficeScan web console and another password to allow unloading and uninstalling the OfficeScan client. (If you choose the same password for both, you will get a warning.) The client unload password is needed to disable real-time scanning on a client computer. Certain CallPilot scenarios (such as installing large software updates or PEPs) work better with real-time scanning disabled. Therefore, CallPilot support personnel may need to know the client unload password so they can temporarily disable real-time scanning so that CallPilot software updates will complete quicker. Click “Next”

Trend Micro OfficeScan

OfficeScan Client Installation

The same installation path will be used for installing the OfficeScan client to all the computers that the OfficeScan server will manage. Please type the installation path below.
Warning: The installation path cannot be changed after setup is complete.

C:\Program Files\Trend Micro\OfficeScan Client

Port number: 56688

Security level:

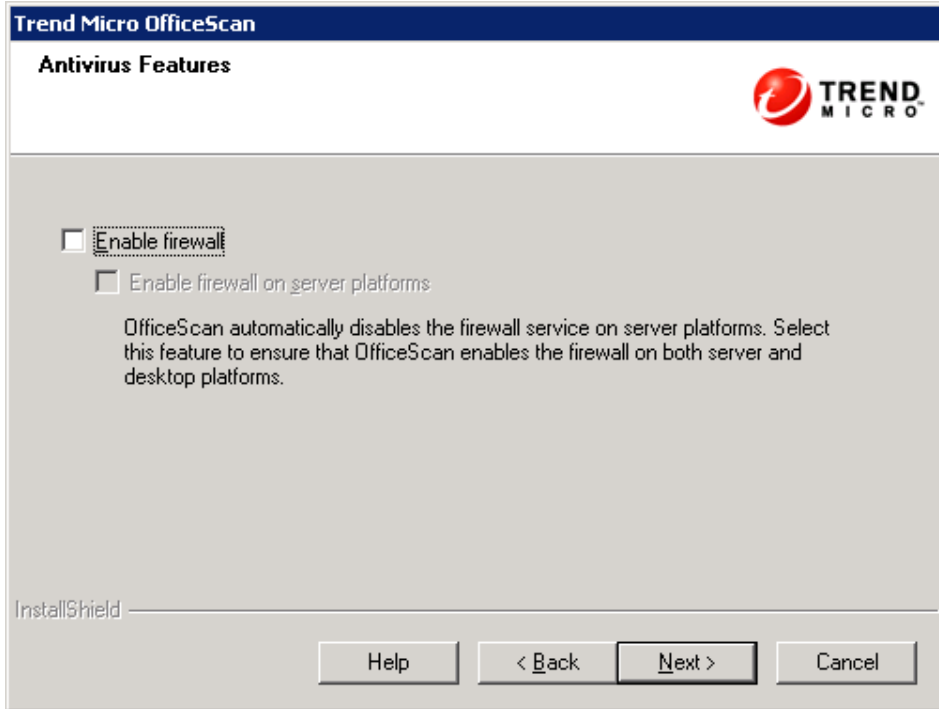
☐ Normal: Assigns the access privileges already configured for the computer's Program Files and registry files to OfficeScan client files and registries.

☒ High: Restricts access to OfficeScan client files and registries.

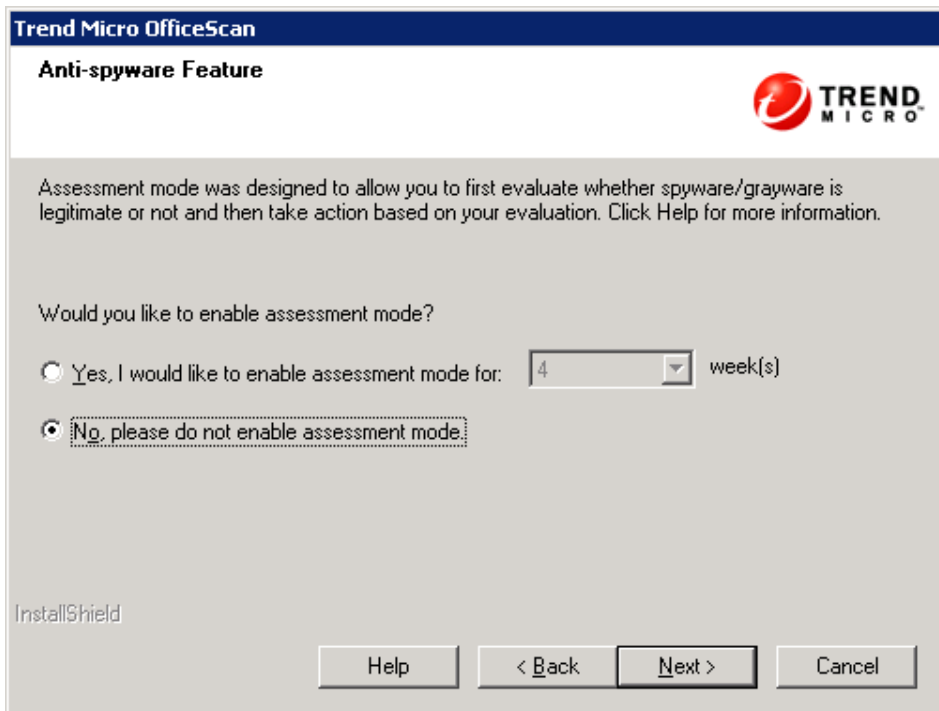
InstallShield

Help < Back Next > Cancel

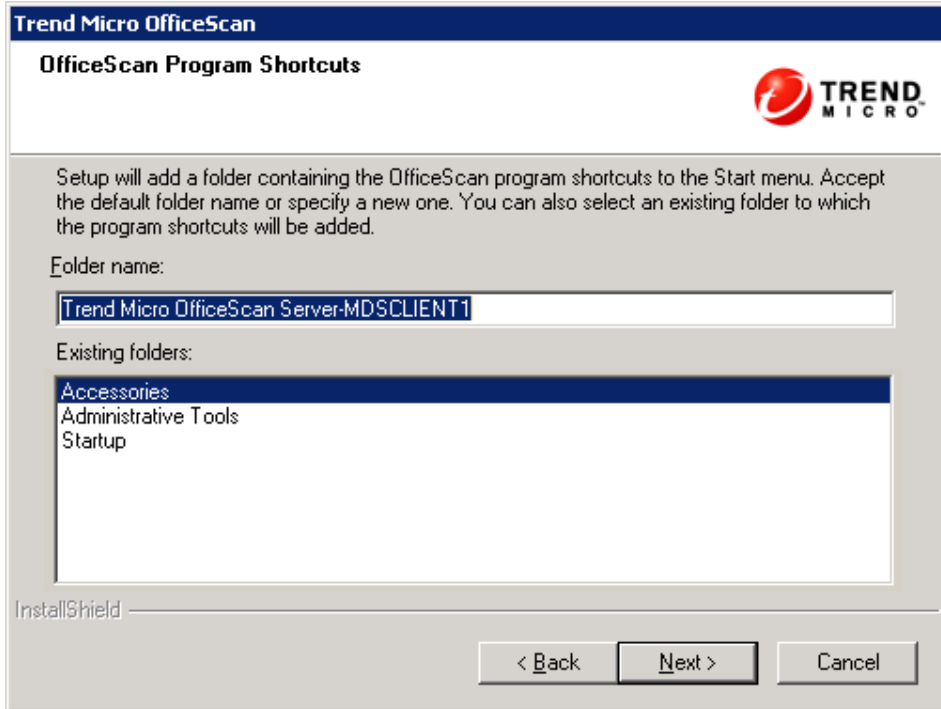
19. Specify the path into which OfficeScan client software will be installed on client machines. Click “Next”.



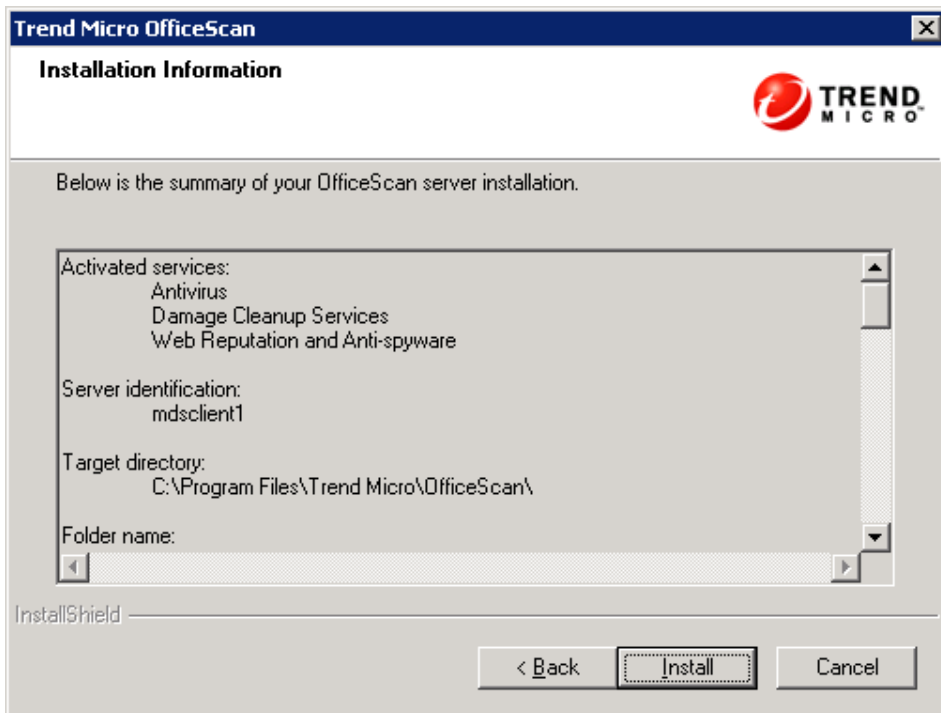
20. Click "Next"



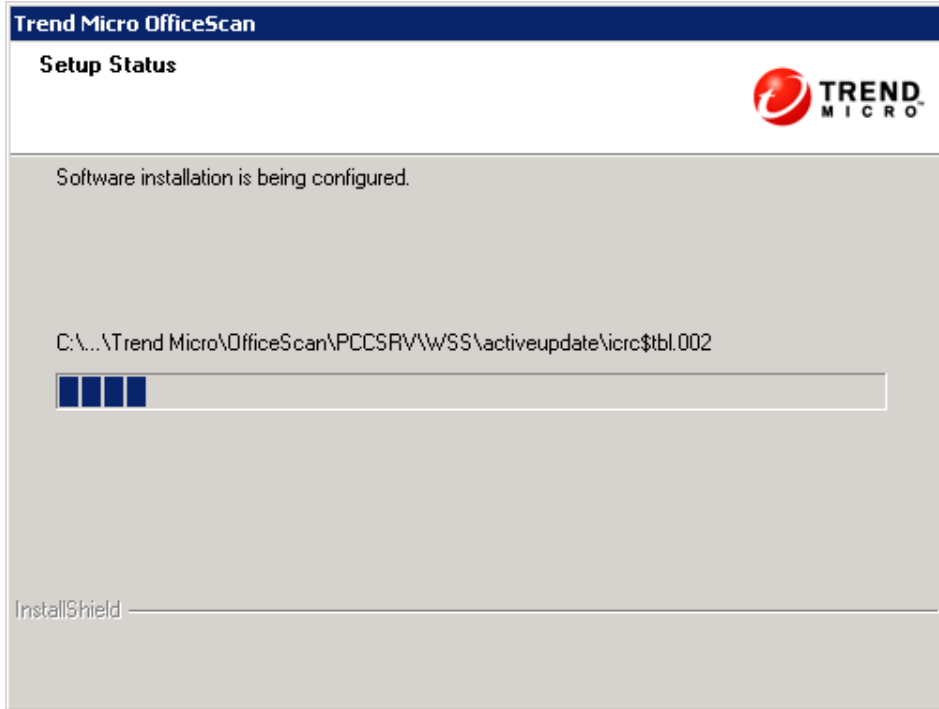
21. You can enable assessment mode. Make your selection and click "Next".



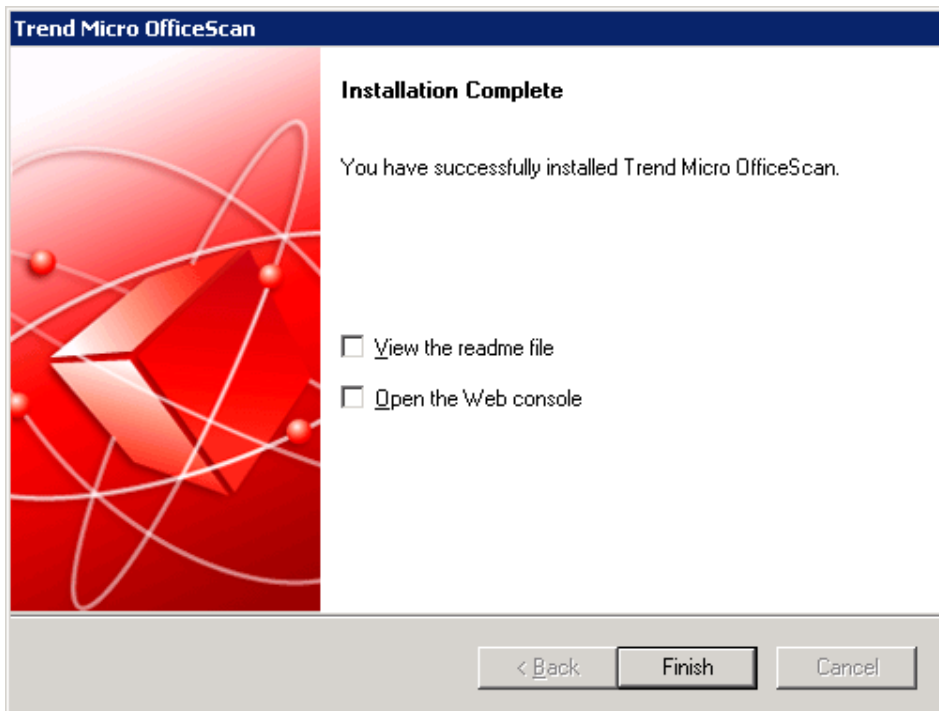
22. Click “Next” (you can change the shortcut location if you want)



23. Click “Install”



24. When installation of the OfficeScan server and OfficeScan client software is complete on your OfficeScan server machine, the following screen will be displayed:



25. Click "Finish". Reboot is not required.

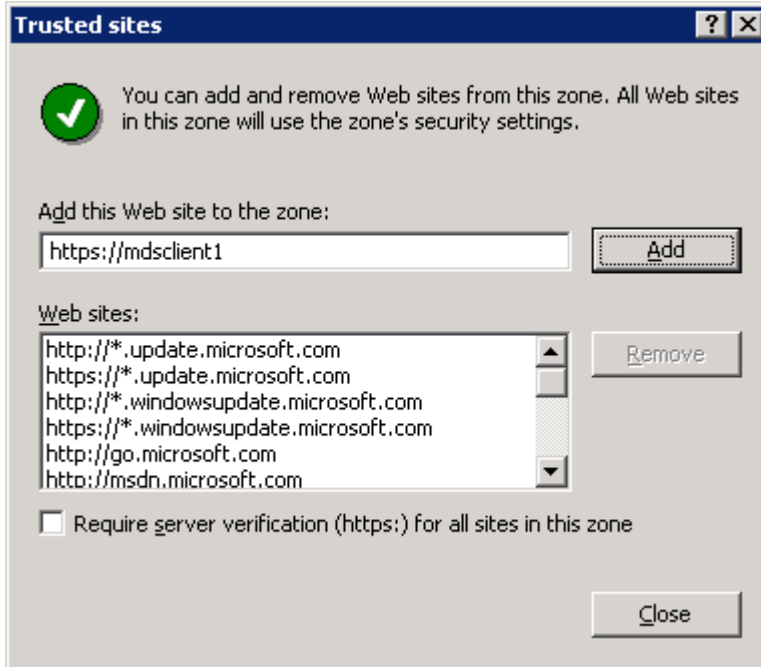
26. Now launch the OfficeScan server Web Console using Start – All Programs – Trend Micro OfficeScan server – OfficeScan Web Console. Depending on the Windows security settings on the OfficeScan server machine, you may get the following security alerts:



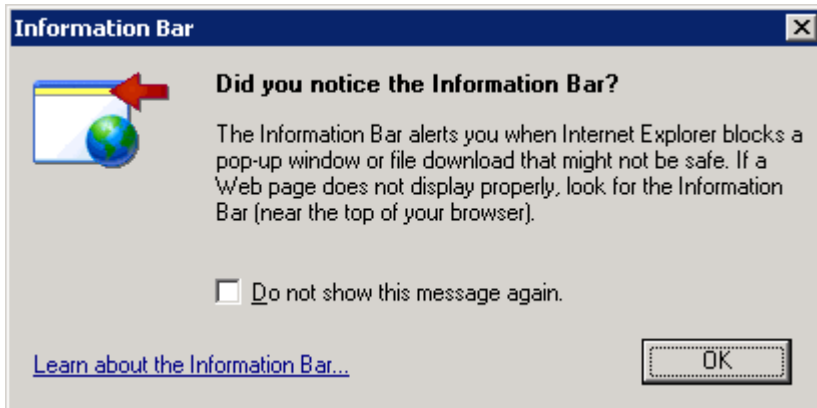
27. If you get this security alert, click "Yes" to accept the certificate.



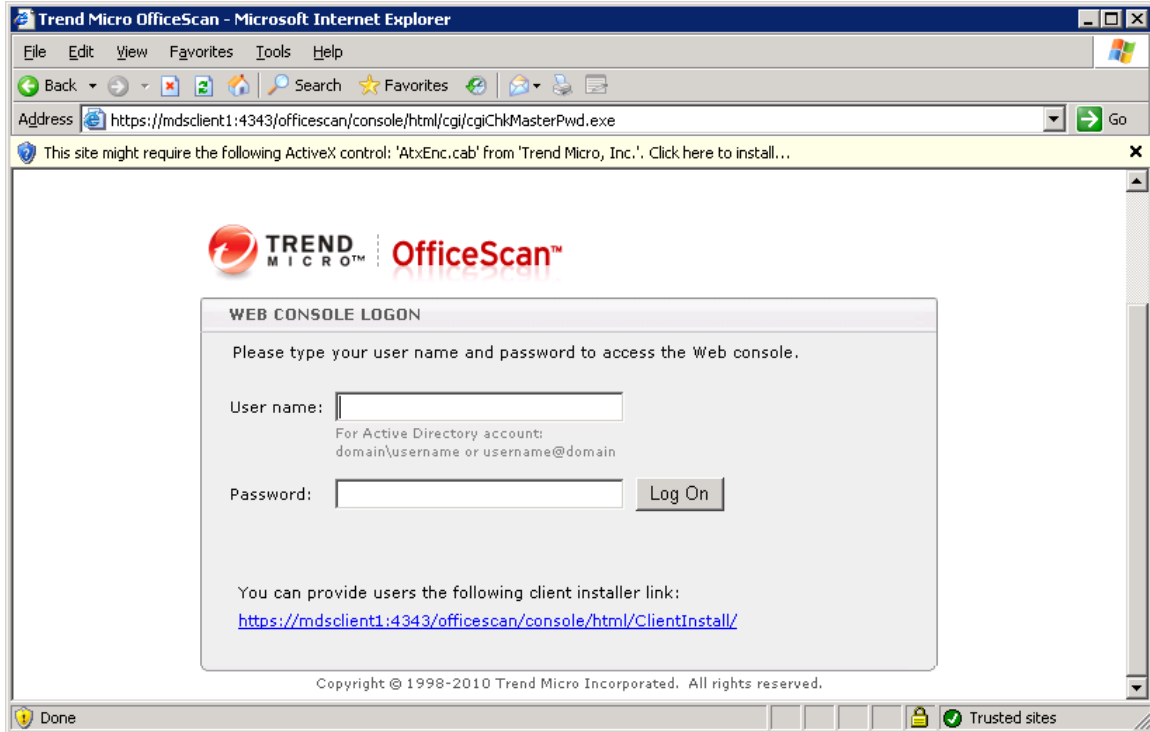
28. If you get this warning, Click "Add" to add the OfficeScan server web site to your list of trusted sites.



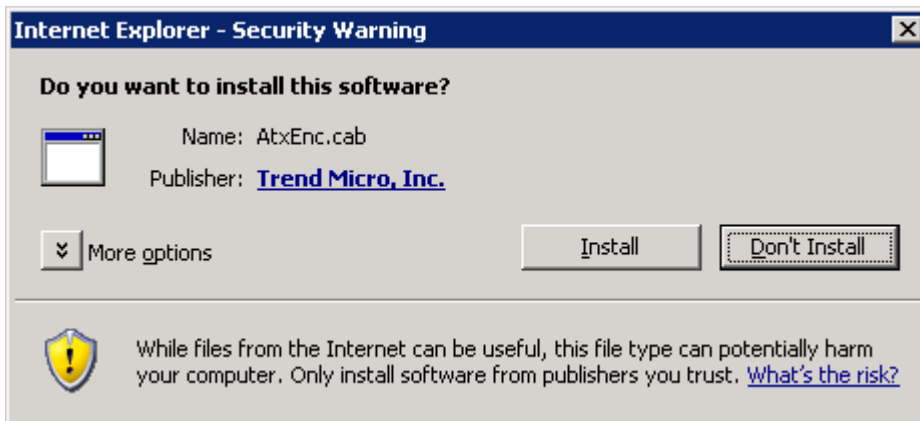
29. “Add” then click “Close”. Then you will probably be asked to install some needed ActiveX controls”



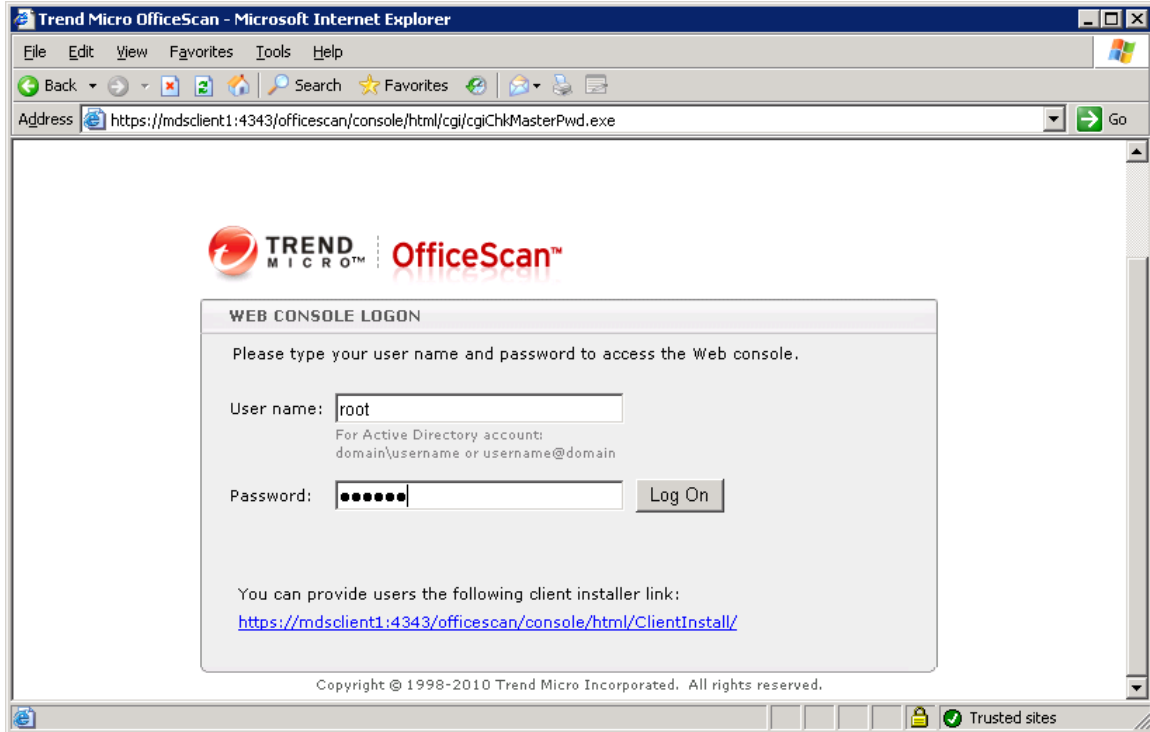
30. Click “OK”, then click in the Information Bar to install the needed ActiveX component



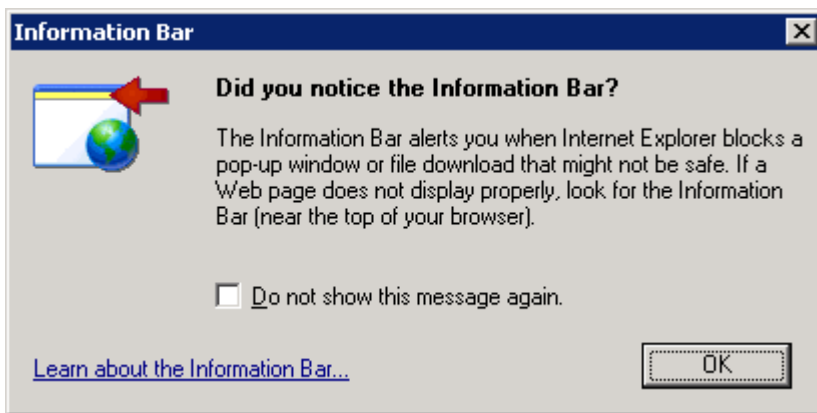
31. Click in the Information Bar to install it



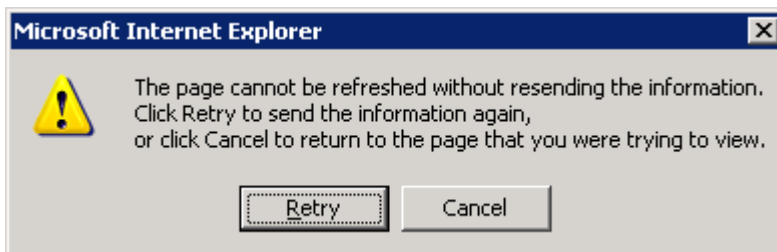
32. Click "Install"



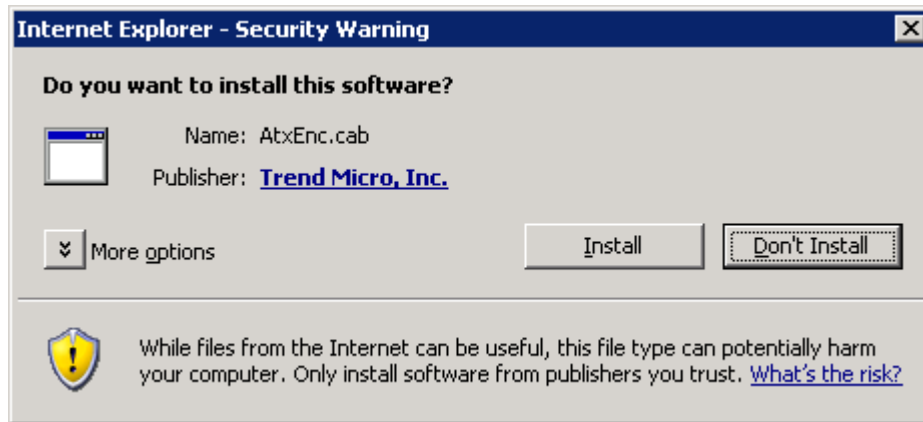
33. Enter standard user name “root” and the password you provided earlier. You may then have to install an additional ActiveX component



34. Click “OK”, then click in the Information Bar to install another needed ActiveX component

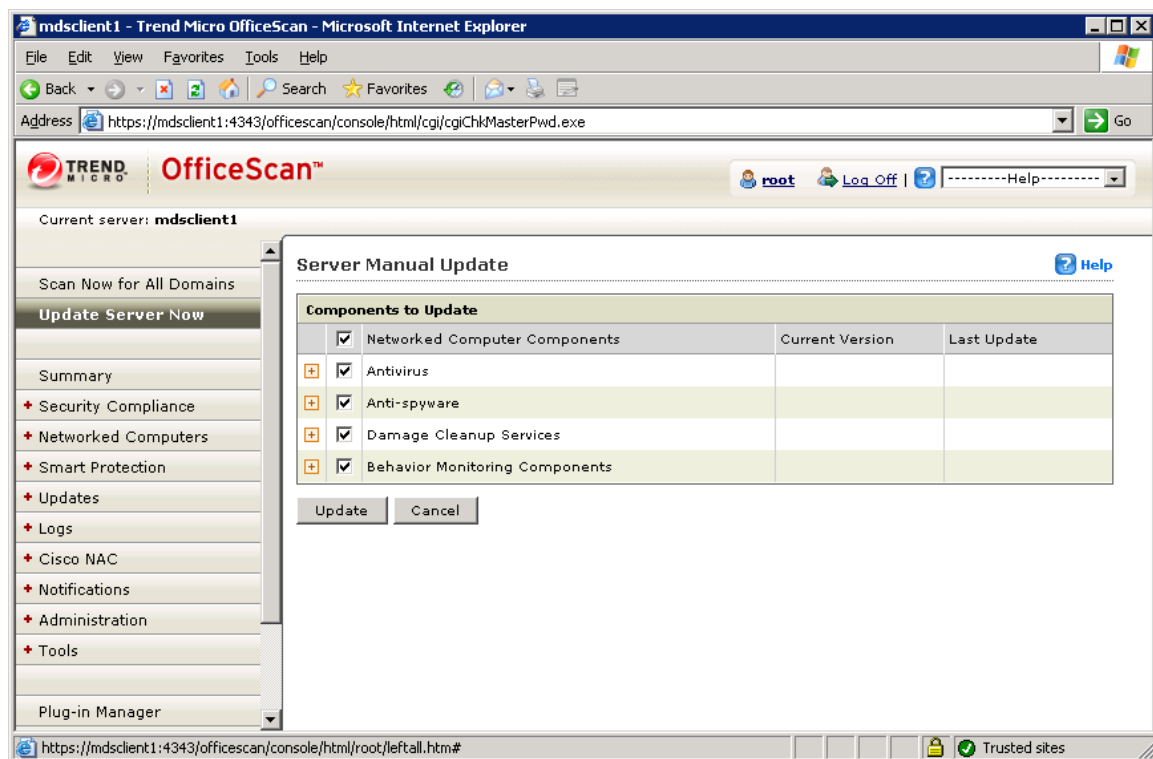


35. If you get this message, click “Retry”

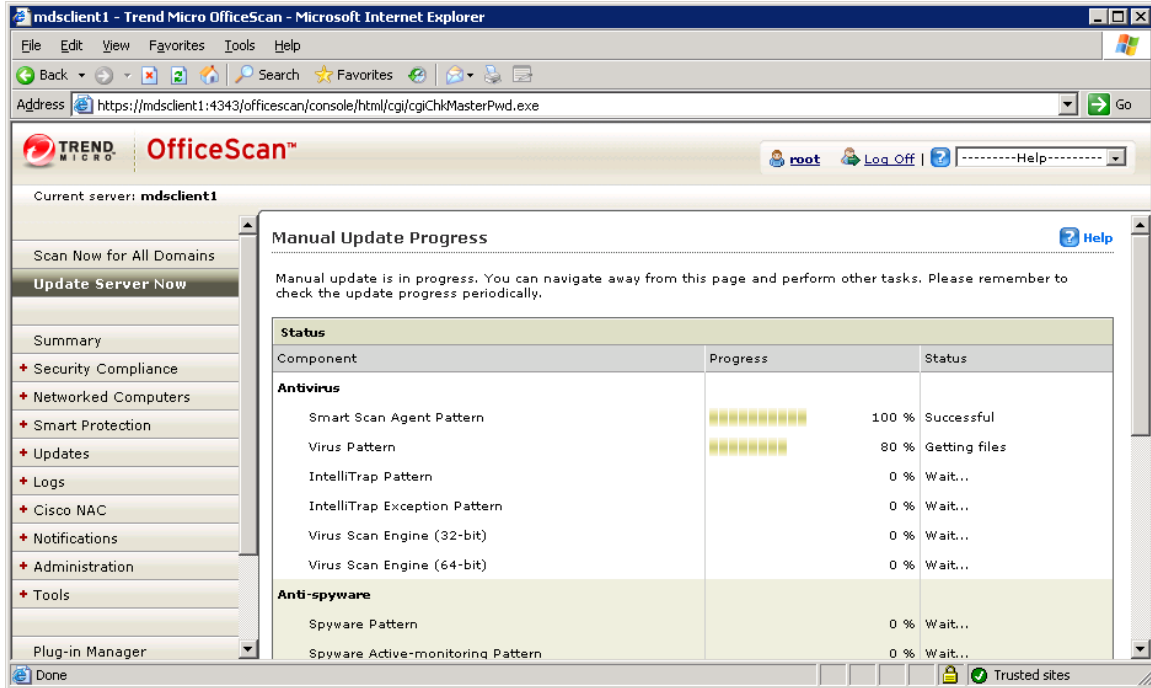


36. Click “Install”

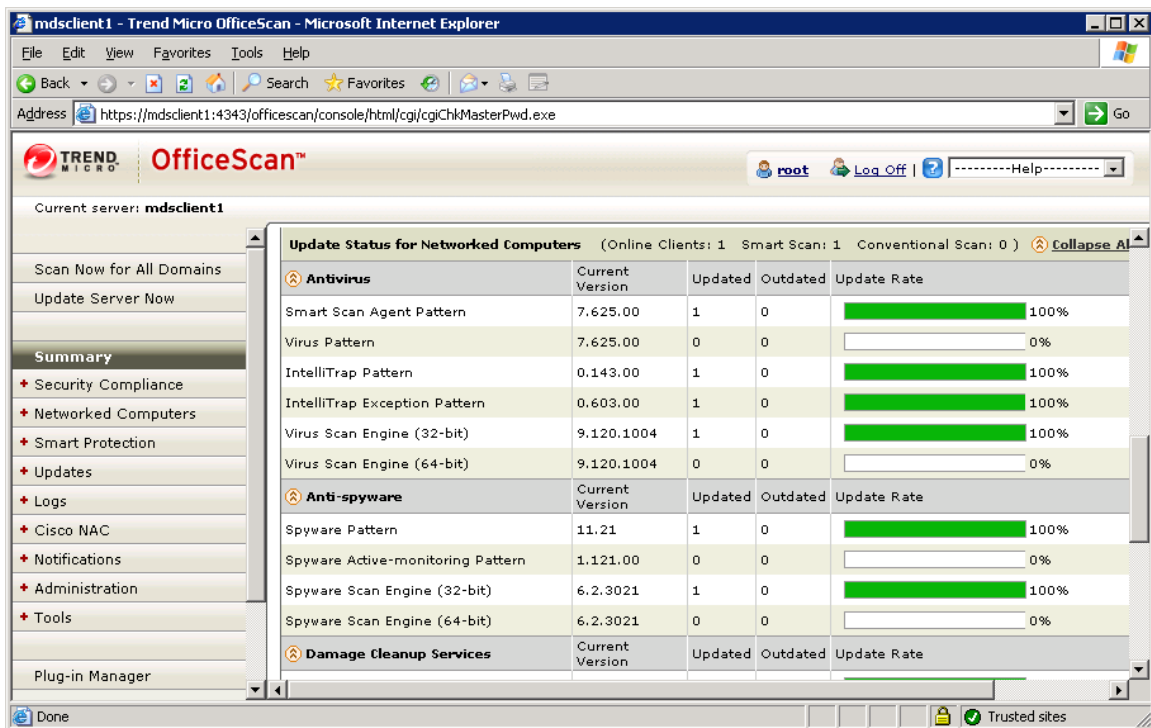
37. On the left side of the OfficeScan Web console page, Click “Update Server Now” to update the antivirus “patterns” (definitions).



38. Check all the components under “Components to Update”. Then click “Update”.

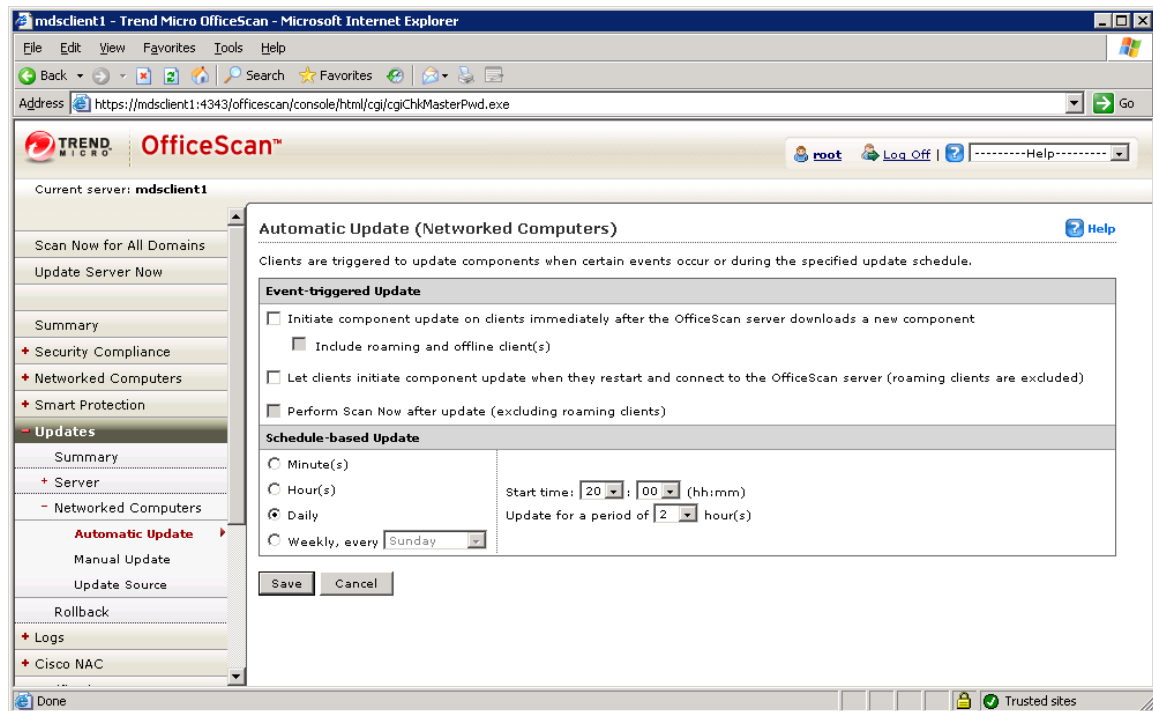


39. When the update is complete, click “Summary” on the left to check that all the needed updates succeeded



40. Check that no needed components are shown as “Outdated”.

41. Select Updates – Networked Computers – Automatic Update. Uncheck “Initiate component update on clients immediately after the OfficeScan server downloads a new component”. Uncheck “Let clients initiate component update when they restart..”. Set up a Schedule-based Update at a time when the CallPilot server is expected to have low traffic. (Problem: the Automatic Update settings seem to apply to all Networked Computers and cannot be specified selectively for only the CallPilot servers. For desktop PCs, which are often powered down at night, the best policy is to distribute updates during the day and to update when a client restarts. For a CallPilot server, however, the server is up 24 hours a day and it is best to distribute updates at night. When a CallPilot server does restart, usually one wants it to come on-line as quickly as possible and therefore getting virus updates at restart is not a good idea.)

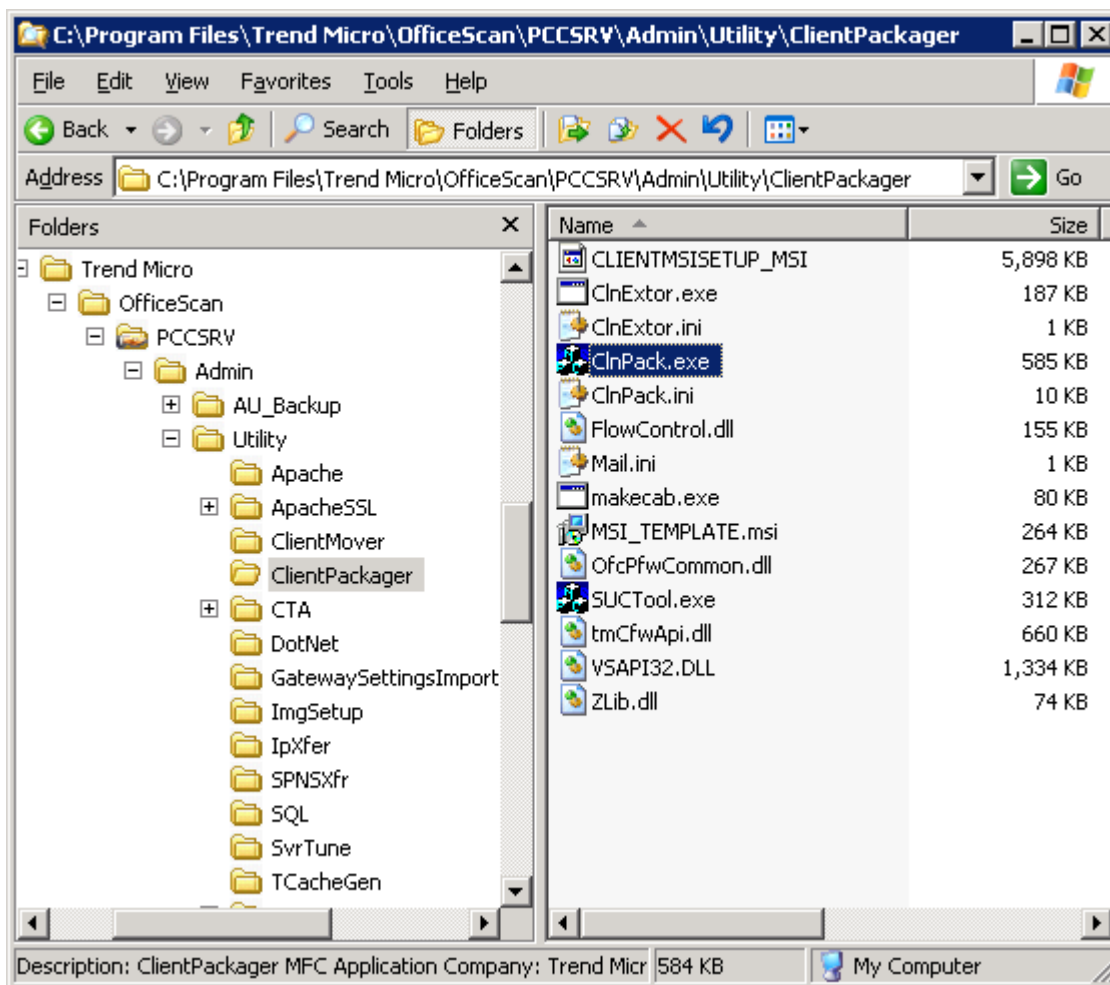


Preparing an OfficeScan Client Package for CallPilot servers and installing it

CallPilot servers require a specific set of parameters for the OfficeScan client. Therefore the client installation for a CallPilot server will not use the same method used for other client PCs being managed by the OfficeScan server. OfficeScan provides a variety of mechanisms for installing on client computers. Avaya recommends that a CallPilot server not be connected to the network until it is fully protected by the latest CallPilot security PEP, all authorized recent hotfixes and an up-to-date anti-virus solution. Therefore, unless the network is very well protected, the OfficeScan client should be installed on CallPilot servers using off-line media such as a CD or (if supported) a USB drive.

The OfficeScan Client Packager utility will be used to create a client package for CallPilot servers, then this can be burned to CD (or written to a USB drive) and physically taken to the CallPilot server for installation.

42. Now launch the Client Package utility (ClnPack.exe) from the location shown below.



Client Packager

Use the Client Packager to create setup or update packages for the OfficeScan client.

Package type: Setup

Windows operating system type: 32-bit

Scan Method: Smart Scan

Options

☐ Silent mode ☐ Force overwrite with latest version

☒ Disable prescan (only for fresh install)

Update agent options

☐ Provide component service

☐ Provide setting service

☐ Provide program service

Client utilities

☐ Outlook Mail Scan ☐ Check Point SecureClient Support

Components

☒ Antivirus ☒ Anti-spyware

☒ Firewall ☒ Damage Cleanup Services

☒ Behavior Monitoring Components

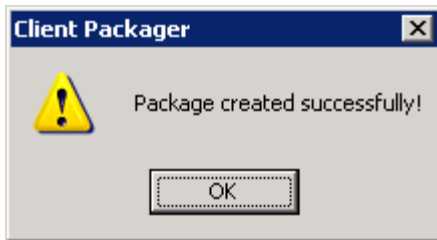
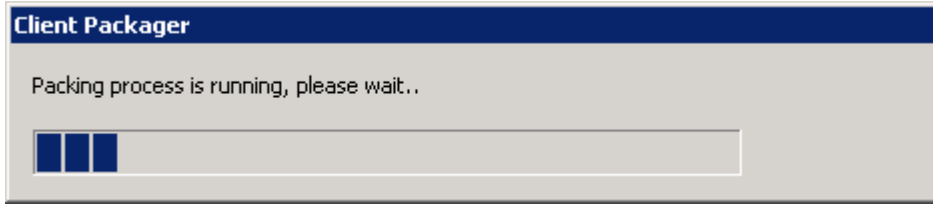
Source file: C:\Program Files\Trend Micro\OfficeScan\PCCSRV\ofcscan.ini

Output file: C:\temp\OfficeScanClientForCP.exe

Create Close

Note: For 201i servers it is recommended to use “Disable prescan” option. The 201i server does not have required resources to perform PreScan within the limit of 5-minute time interval. When PreScan takes more than 5 minutes, the setup program will not install successfully.

43. Specify a location and file name for the CallPilot OfficeScan Client Installation package. (Note: CallPilot servers must not be used as “Update Agents” to distribute virus patterns since this adds extra load onto them) Then Click “Create”.



44. Click OK, then Close.

45. Write the Client Install package to CD or USB drive and take it to the CallPilot server. Execute it on the CallPilot server to install the OfficeScan client. The package will include the current virus definitions that are installed on the OfficeScan server.

Configuring OfficeScan on a CallPilot server

Now that OfficeScan has been installed on the CallPilot server, if the latest CallPilot security PEP and other authorized hotfixes have also been installed, the CallPilot server is adequately protected and the CLAN cable can be reconnected. Be sure that the CLAN networking parameters have been fully configured, including any appropriate DNS settings.

Now the CallPilot server will show up on the OfficeScan server management page and can be managed from there.

46. Access the OfficeScan server Web console. This can be done from the OfficeScan server itself (Start – All Programs – Trend Micro OfficeScan Server – OfficeScan Web Console) or by browsing to the OfficeScan server from any other desktop on the LAN (Use URL <https://webserver:4343/officescan/console/html/cgiChkMasterPwd.exe> - where “webserver” is the DNS name or IP address of the OfficeScan server machine). Log in using the password.

The screenshot displays the Trend Micro OfficeScan Web Console. The browser window title is "mdsclient1 - Trend Micro OfficeScan - Microsoft Internet Explorer". The address bar shows "https://mdsclient1:4343/officescan/console/html/cgiChkMasterPwd.exe". The interface includes a left sidebar with navigation options: Summary, Security Compliance, Networked Computers, Smart Protection, Updates, Logs, Cisco NAC, Notifications, Administration, Tools, and Plug-in Manager. The main content area shows "Activated services: Desktop/Server Antivirus, Desktop/Server Web Reputation and Anti-spyware, File Reputation, Damage Cleanup Services" and a "Status summary as of 11/16/2010 12:07:46". The "Networked Computers" section displays a pie chart and a table with columns: Status, Smart Scan, Conventional Scan, and Total. The table shows 1 Online, 0 Offline, and 0 Roaming computers. The "Detection Status" table shows 0 detections for Virus/Malware and Spyware/Grayware. The "Outbreak Status" section shows "View Top 10 Security Risk Statistics" and a table with columns: Type, Current Outbreak, and Last Outbreak. The "Update Status for Networked Computers" section shows "Online Clients: 1 Smart Scan: 1 Conventional Scan: 0" and a table with columns: Component, Current Version, Updated, Outdated, and Update Rate. The table lists updates for Antivirus and Anti-spyware components, all showing 100% update rate.

47. On the left, select “Networked Computers”, then “Client Management”. Expand the tree under “OfficeScan server” to see the computers being managed. (Note: if there are multiple CallPilot servers, it is possible to use the Web Console “Manage Client Tree” menu to create a separate “Domain” for them. Please be sure the settings are still set correctly.)

mdsclient1 - Trend Micro OfficeScan - Microsoft Internet Explorer

Address: https://mdsclient1:4343/officescan/console/html/cgiChkMasterPwd.exe

TREND MICRO OfficeScan

Current server: mdsclient1

Scan Now for All Domains
Update Server Now

Summary
Security Compliance
Networked Computers

Client Management

Client Grouping
Global Client Settings
Computer Location
Client Installation
Connection Verification
Outbreak Prevention
Smart Protection
Updates
Logs
Cisco NAC
Notifications
Administration
Tools

Plug-in Manager

Client Management

Select domains or computers from the client tree, and then select one of the tasks provided above the client tree.

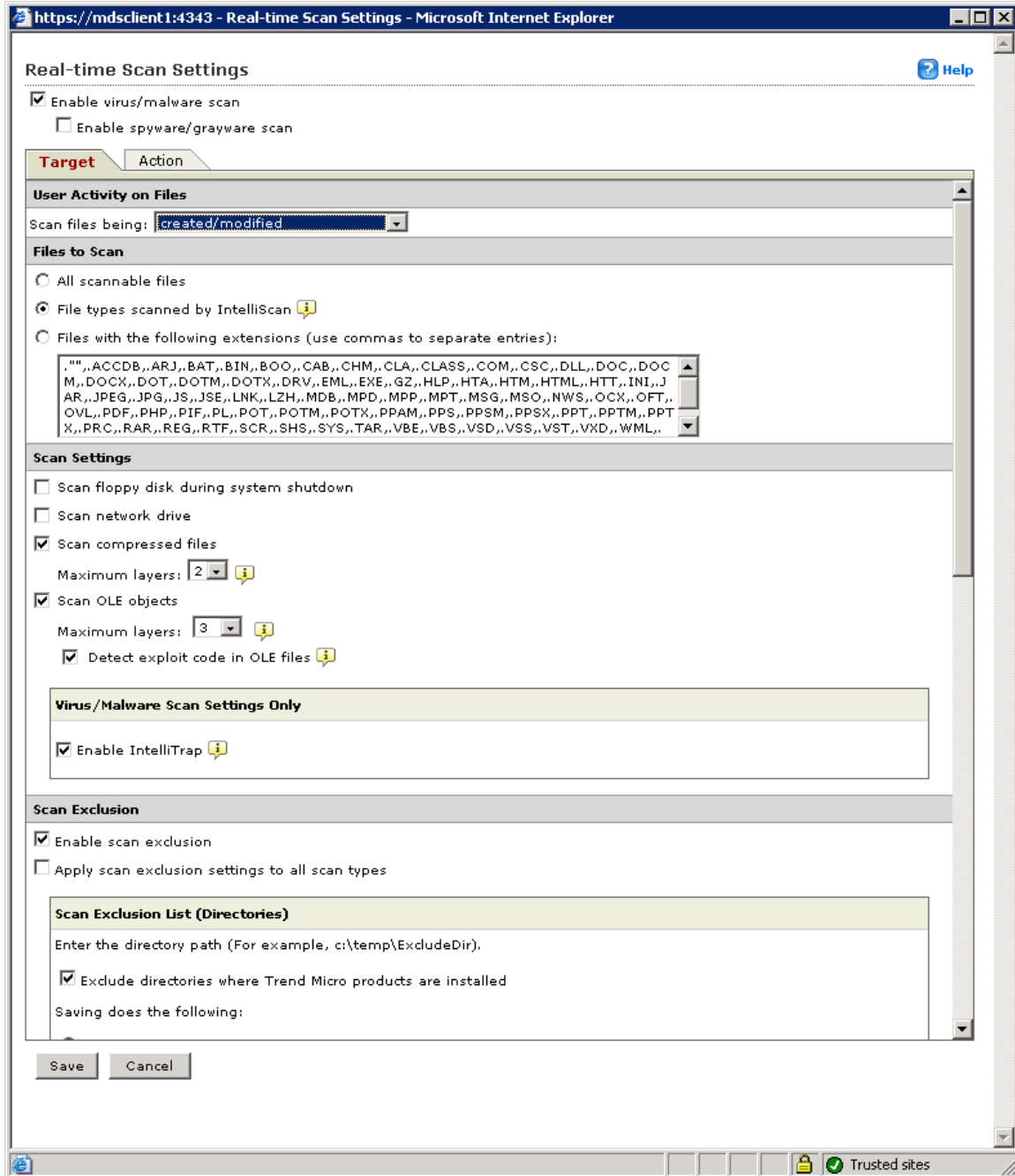
Search for computers: Search Advanced search

Client tree view: Update view Server GUID: 657de87a-1f96-4cf1-ae90-1f35c6ed7997

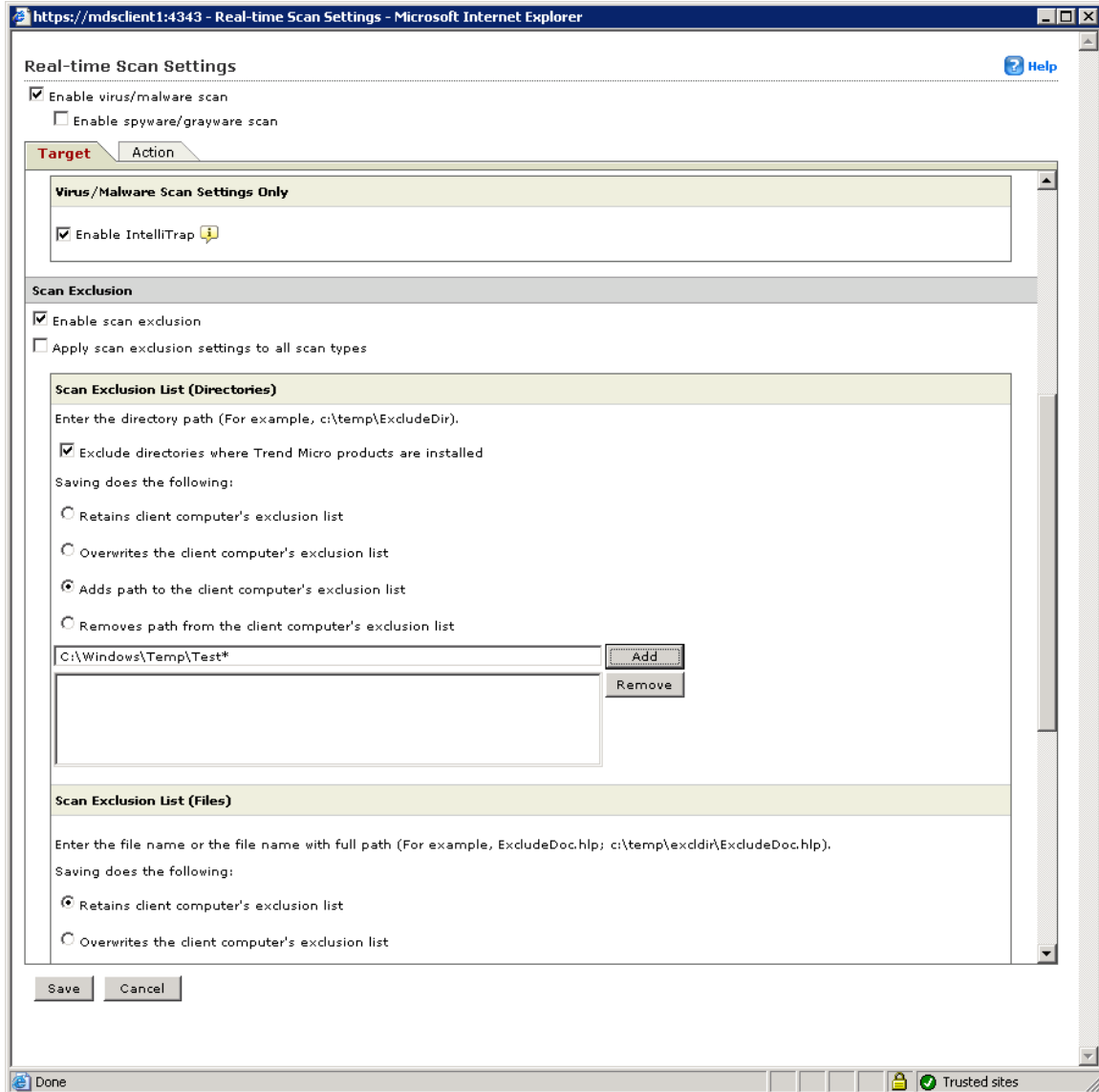
Domain/Computer	IP Address	List	Domain Name	Connection	GUID
CP201_2	192.1...	47885	Workgroup\	Online	2ecd2508-1a60-4b9e-9af...
MDSCLIENT1	192.1...	47885	Workgroup\	Online	bb837bf0-fcc5-41c1-bb4f...

Number of clients: 2 Clients using Smart scan: 2 Clients using Conventional scan: 0

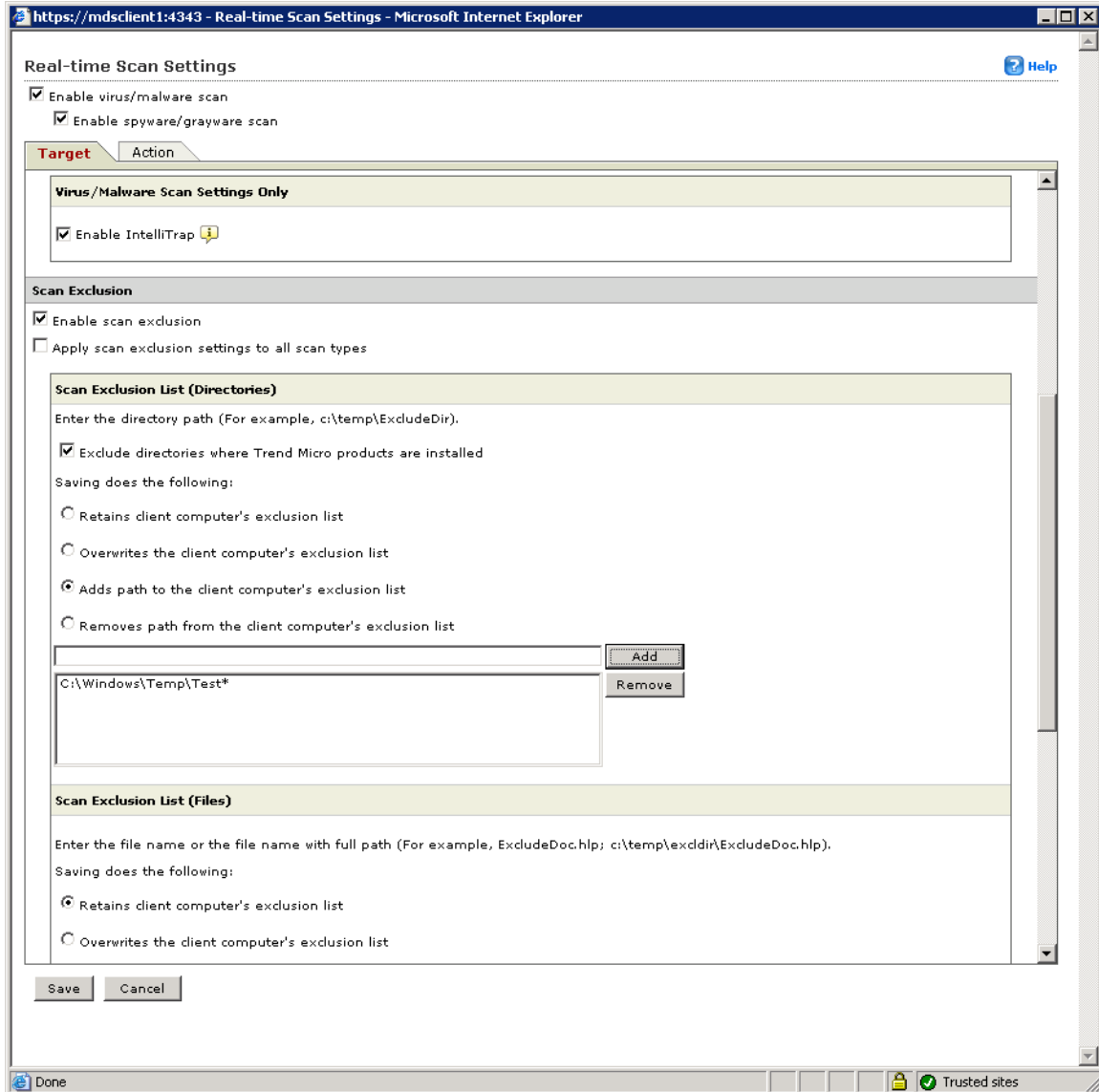
48. Click to select the CallPilot server(s) and use the “Settings” menu to select “Real-time Scan Settings”



49. Uncheck “Enable spyware/grayware scan”. Select “Scan files being create/modified”. (Scanning files every time they are retrieved will add extra overhead onto the CallPilot server and may result in performance problems.) Scroll down.

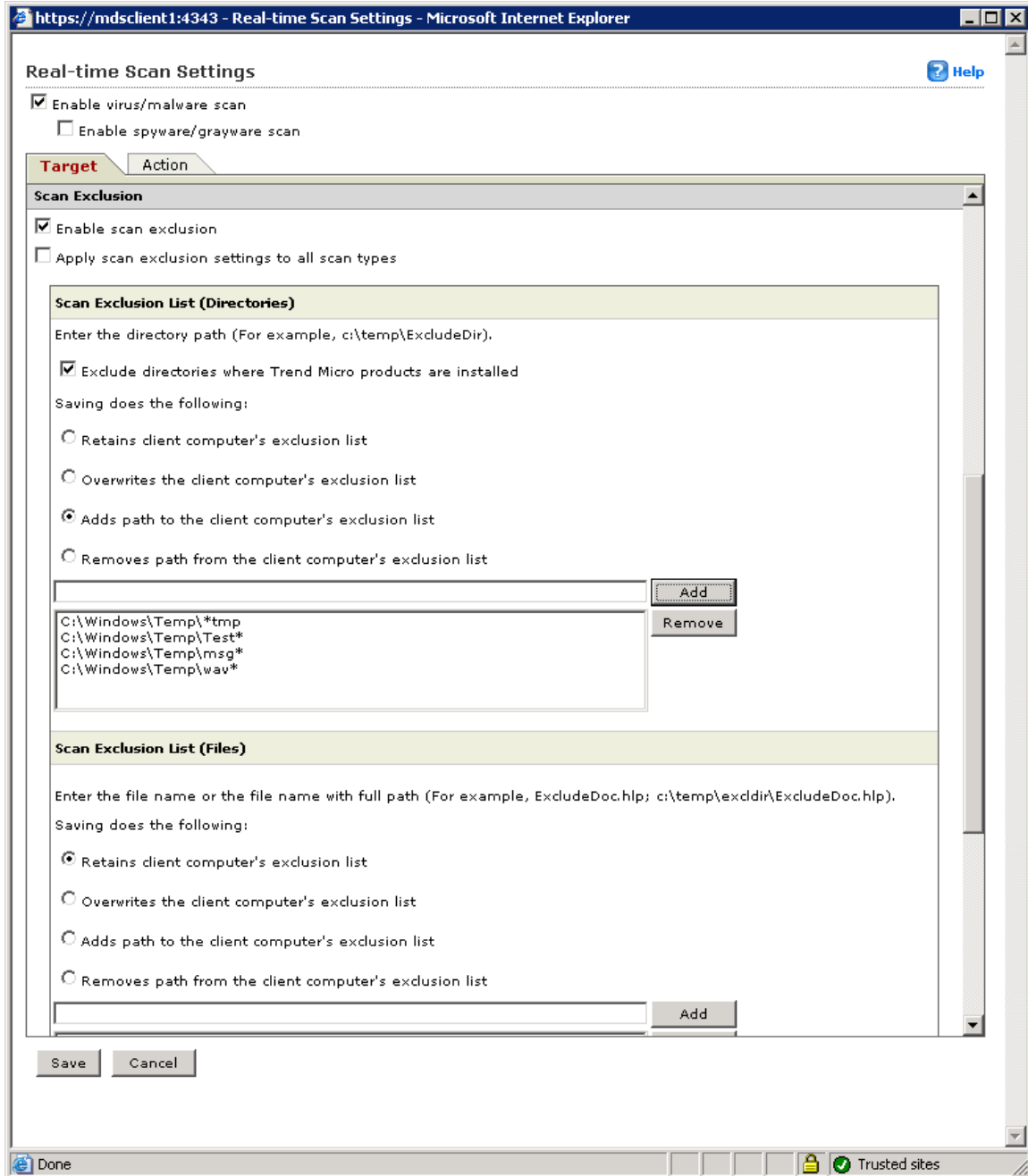


50. Under “Scan Exclusion List (Directories)” select “Adds path to the client computer's exclusion list”. Type “C:\Windows\Temp\Test*” and click “Add”.

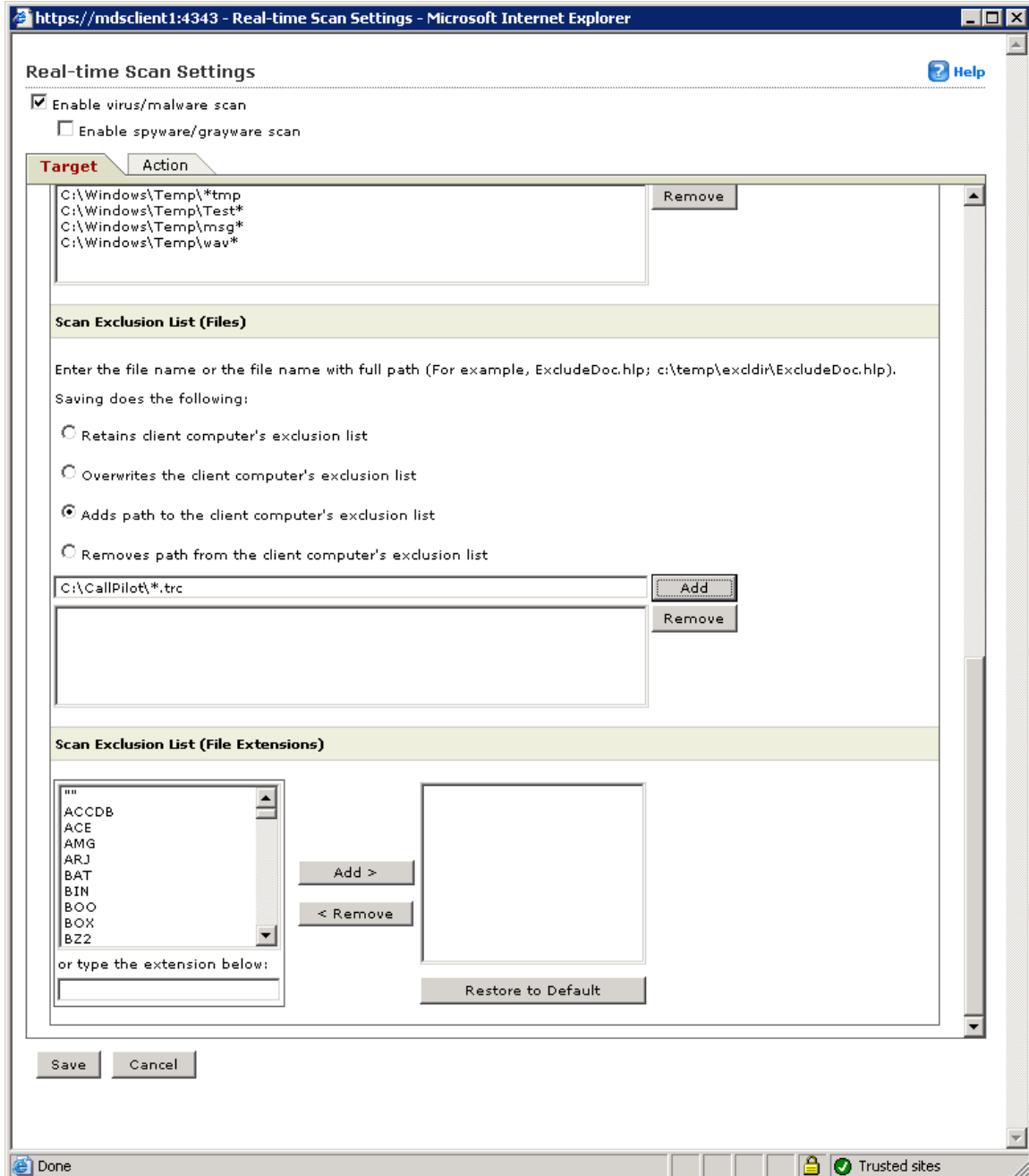


51. Add the following exclusions in the same way:

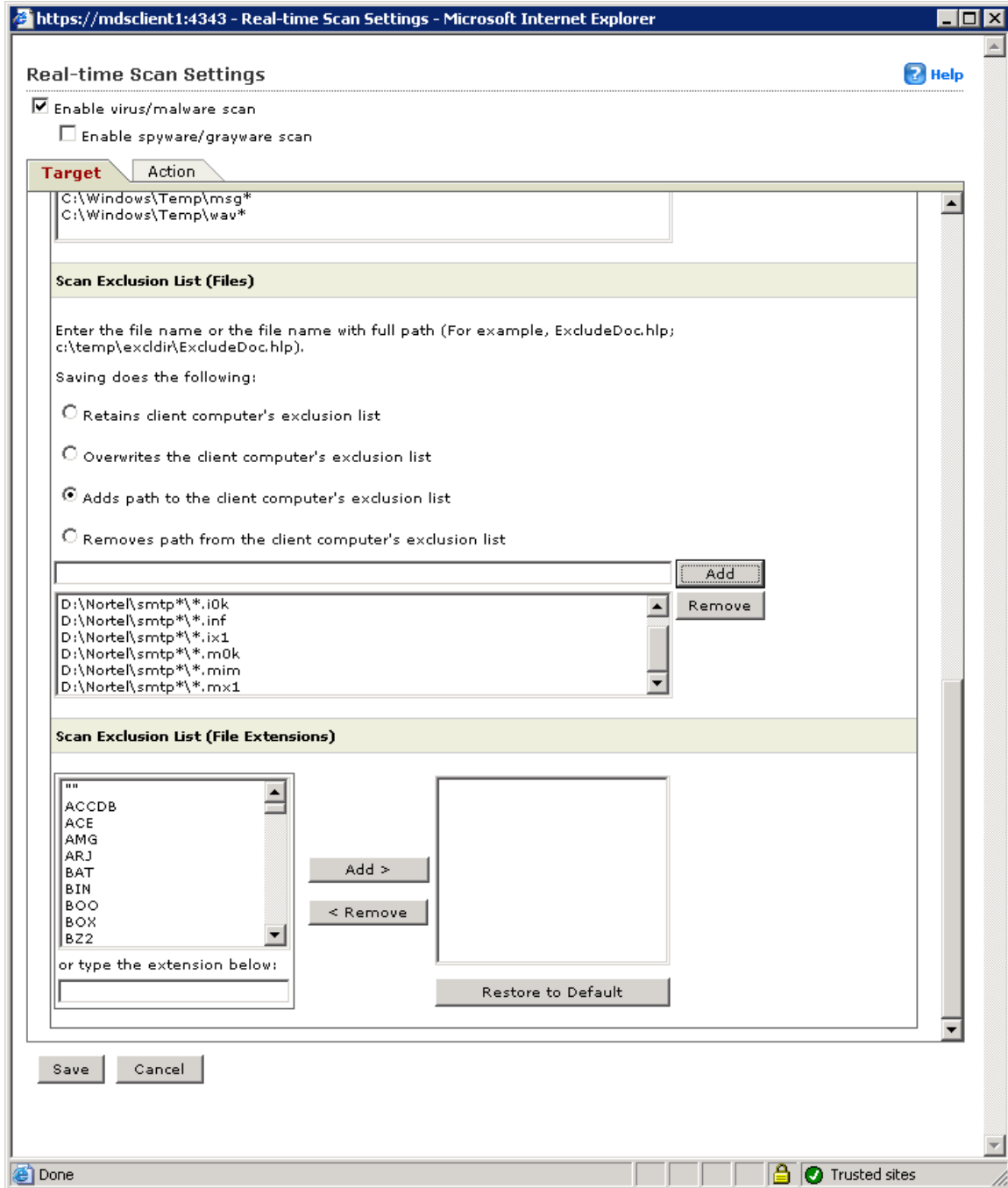
C:\Windows\Temp\wav*
 C:\Windows\Temp*tmp
 C:\Windows\Temp\msg*



52. Scroll down.



53. Under “Scan Exclusion List (Files)” select “Adds path to the client computer's exclusion list”. Type “C:\CallPilot*.trc” and click “Add”.



54. Add the following exclusions in the same way:

D:\Nortel\smtp**.mim
 D:\Nortel\smtp**.inf
 D:\Nortel\smtp**.mOk (that's letter m, number zero, letter k)
 D:\Nortel\smtp**.iOk (that's letter i, number zero, letter k)
 D:\Nortel\smtp**.mx1
 D:\Nortel\smtp**.ix1

Also, on CallPilot HA systems the following additional exclusion should be specified:

“D:\Program Files\EMC AutoStart\<Domain Name>_<Computer Name>” (Where Domain Name is the name associated with the HA pair and Computer Name is the name of the specific node within that pair.)

55. Select the “Action” tab

https://mdsclient1:4343 - Real-time Scan Settings - Microsoft Internet Explorer

Real-time Scan Settings

☒ Enable virus/malware scan
☐ Enable spyware/grayware scan

Target **Action**

Virus/Malware

☒ Use **ActiveAction** ⓘ
☐ Customize action for probable virus/malware: Quarantine

☐ Use the same action for all virus/malware types
(If you choose Clean, specify the second action OfficeScan will take if cleaning fails)

Type	1st Action	2nd Action
All Types	Clean	Quarantine

☐ Use a specific action for each virus/malware type

Type	1st Action	2nd Action
Joke	Quarantine	
Trojan	Quarantine	
Virus	Clean	Quarantine
Test Virus	Deny access	
Packer	Quarantine	
Probable Virus/Malware	Quarantine	
Others	Clean	Quarantine

Quarantine directory: HTTP://mdsclient1

☒ Back up files before cleaning
☒ Display a notification message on the client computer when virus/malware is detected
☒ Display a notification message on the client computer when probable virus/malware is detected
☐ Enable system clean up for probable virus/malware

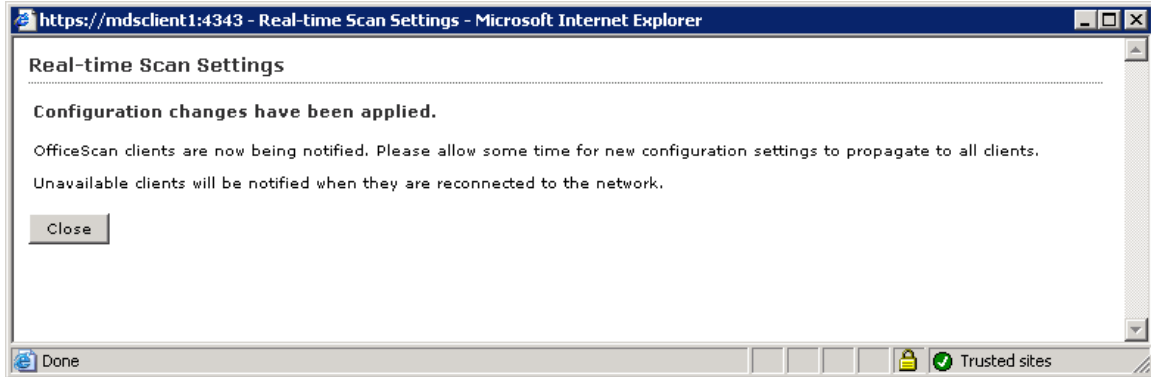
Spyware/Grayware

☒ Clean: OfficeScan will terminate processes or delete registries, files, cookies and shortcuts.
☐ Deny access
☒ Display a notification message on the client computer when spyware/grayware is detected

Save Cancel

Done Trusted sites

56. Click “Save” to save the modified client settings.



57. Click "Close"

58. With the CallPilot server(s) still selected, use the "Settings" menu to select "Privileges and Other Settings".

https://mdscient1:4343 - Privileges and Other Settings - Microsoft Internet Explorer

Privileges and Other Settings Help

Privileges Other Settings

Roaming Privilege

☐ Enable roaming mode

Scan Privileges

Allow users to do the following:

☐ Configure Manual Scan settings

☒ Configure Real-time Scan settings

☒ Configure Scheduled Scan settings

Scheduled Scan Privileges

Allow users to do the following:

☒ Postpone Scheduled Scan

☒ Skip and stop Scheduled Scan

Behavior Monitoring Privileges

☐ Display the Behavior Monitoring tab on the client console

Mail Scan Privileges

☒ Display the Mail Scan tab on the client console ?

Toolbox Privileges

☒ Display the Toolbox tab on the client console and allow users to install Check Point SecureClient Support

Proxy Setting Privileges

☒ Allow the client user to configure proxy settings ?

Component Update Privileges

Allow users to do the following:

☒ Perform "Update Now!"

☐ Enable scheduled update ?

Uninstallation

☐ Allow the user to uninstall the OfficeScan client

☒ Require a password for the user to uninstall the OfficeScan client

Password:

Confirm password:

Unloading

☐ Allow the user to unload the OfficeScan client

☒ Require a password for the user to unload the OfficeScan client

Password:

Confirm password:

Done Trusted sites

59. Use the settings shown above to allow local users to Configure Real-time Scan settings, Configure Scheduled Scan settings, Postpone Scheduled Scan, Skip and Stop Scheduled Scan and Perform Update Now. The idea here is to allow an authorized CallPilot support person to adjust settings if needed and to stop a scheduled scan if one starts up at a bad time or during a maintenance window. Note that certain CallPilot operations (such as large software updates or PEP installs) work faster and better with real-time scanning disabled. Therefore, CallPilot support personnel may require the ability to temporarily disable real-time scanning by "unloading" the OfficeScan client. Therefore the password specified here under "Unloading", may need to be given to CallPilot support.

60. Click “Save”

61. With the CallPilot servers(s) still selected, use the “Settings” menu to select “Scheduled Scan Settings”.

https://mdsclient1:4343 - Scheduled Scan Settings - Microsoft Internet Explorer

Scheduled Scan Settings [Help](#)

☒ Enable virus/malware scan
☐ Enable spyware/grayware scan

Target **Action**

Schedule

☐ Daily
☒ Weekly, every **Sunday** Start time: **20** : **00** (hh:mm)
☐ Monthly, on day **01**

Files to Scan

☐ All scannable files
☒ File types scanned by IntelliScan
☐ Files with the following extensions (use commas to separate entries):
",,ACCCDB,,ARJ,,BAT,,BIN,,BOO,,CAB,,CHM,,CLA,,CLASS,,COM,,CSC,,DLL,,DOC,,DOC
M,,DOCX,,DOT,,DOTM,,DOTX,,DRV,,EML,,EXE,,GZ,,HLP,,HTA,,HTM,,HTML,,HTT,,INI,,J
AR,,JPEG,,JPG,,JS,,JSE,,LNK,,LZH,,MDB,,MPD,,MPP,,MPT,,MSG,,MSO,,NWS,,OCX,,OFT,,
OVL,,PDF,,PHP,,PIF,,PL,,POT,,POTM,,POTX,,PPAM,,PPS,,PPSM,,PPSX,,PPT,,PPTM,,PPT
X,,PRC,,RAR,,REG,,RTF,,SCR,,SHS,,SYS,,TAR,,VBE,,VBS,,VSD,,VSS,,VST,,VXD,,WML,,

Scan Settings

☒ Scan compressed files
Maximum layers: **2**
☒ Scan OLE objects
Maximum layers: **3**
☒ Detect exploit code in OLE files

Virus/Malware Scan Settings Only

☒ Scan boot area

CPU Usage

If your client computers run CPU-intensive applications, you may want OfficeScan to pause between file scans to free up CPU resources.

☐ High: scan files one after another without pausing
☐ Medium: pause between file scans if CPU consumption is higher than 50%, and do not pause if 50% or lower
☒ Low: pause between file scans if CPU consumption is higher than 20%, and do not pause if 20% or lower

Scan Exclusion

Save **Cancel**

Done Trusted sites

62. Enable a virus/malware scan and set up a regular scheduled scan at a time when load on the CallPilot server is expected to be very low. Set “CPU Usage” to “Low” to minimize the performance impact on any callers who do access the system during a scan. A scheduled scan takes about 75 minutes on a CallPilot 201i server.

63. Scroll down.

https://mdsclient1:4343 - Scheduled Scan Settings - Microsoft Internet Explorer

Scheduled Scan Settings [Help](#)

☒ Enable virus/malware scan
☐ Enable spyware/grayware scan

Target **Action**

☒ Low: pause between file scans if CPU consumption is higher than 20%, and do not pause if 20% or lower

Scan Exclusion

☒ Enable scan exclusion
☐ Apply scan exclusion settings to all scan types

Scan Exclusion List (Directories)

Enter the directory path (For example, c:\temp\ExcludeDir).

☒ Exclude directories where Trend Micro products are installed

Saving does the following:

☒ Retains client computer's exclusion list
☐ Overwrites the client computer's exclusion list
☐ Adds path to the client computer's exclusion list
☐ Removes path from the client computer's exclusion list

Scan Exclusion List (Files)

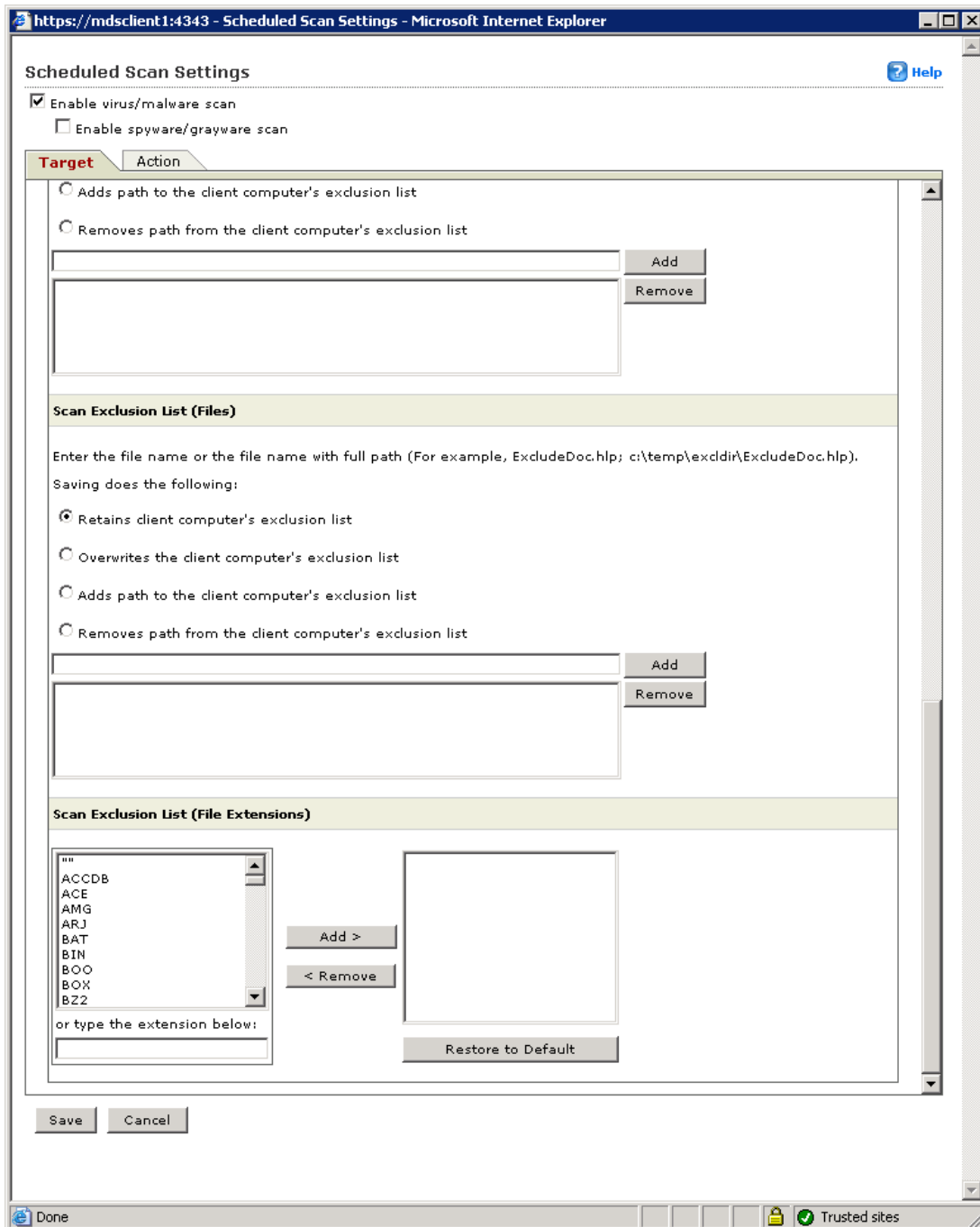
Enter the file name or the file name with full path (For example, ExcludeDoc.hlp; c:\temp\excldir\ExcludeDoc.hlp).

Saving does the following:

☒ Retains client computer's exclusion list
☐ Overwrites the client computer's exclusion list
☐ Adds path to the client computer's exclusion list
☐ Removes path from the client computer's exclusion list

Done

64. Scroll down.



65. Select the “Action” tab.

https://mdsclient1:4343 - Scheduled Scan Settings - Microsoft Internet Explorer

Scheduled Scan Settings [Help](#)

☒ Enable virus/malware scan
☐ Enable spyware/grayware scan

Target **Action**

Virus/Malware

☒ Use **ActiveAction** ⓘ
☐ Customize action for probable virus/malware: Quarantine

☐ Use the same action for all virus/malware types
 (If you choose Clean, specify the second action OfficeScan will take if cleaning fails)

Type	1st Action	2nd Action
All Types	Clean	Quarantine

☐ Use a specific action for each virus/malware type

Type	1st Action	2nd Action
Joke	Quarantine	
Trojan	Quarantine	
Virus	Clean	Quarantine
Test Virus	Pass	
Packer	Quarantine	
Probable Virus/Malware	Quarantine	
Others	Clean	Quarantine

Quarantine directory: HTTP://mdsclient1

☒ Back up files before cleaning
☒ Display a notification message on the client computer when virus/malware is detected
☒ Display a notification message on the client computer when probable virus/malware is detected
☐ Enable system clean up for probable virus/malware

Spyware/Grayware

☒ Clean: OfficeScan will terminate processes or delete registries, files, cookies and shortcuts.
☐ Pass: OfficeScan will log the spyware/grayware detection for assessment.
☒ Display a notification message on the client computer when spyware/grayware is detected

Save Cancel

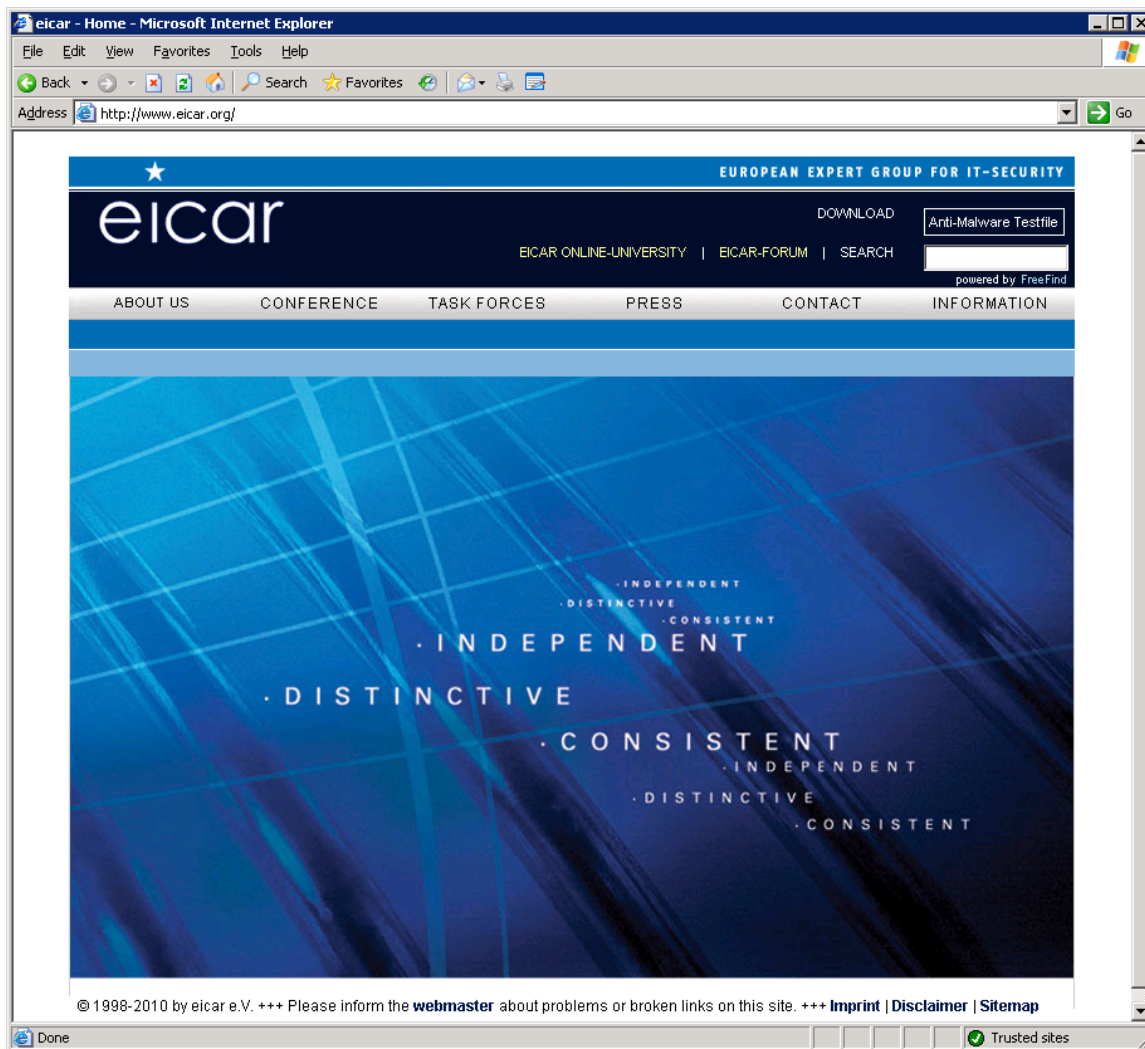
Done Trusted sites

66. The default Actions are acceptable. Note that AV software sometimes has “false positives” where legitimate files are erroneously flagged as malware. If this happens and an important CallPilot file is detected as a virus, it will be necessary to be able to restore the file. Therefore files should not be automatically deleted.

67. Click “Save”.

Testing Trend Micro OfficeScan with the EICAR test virus

Open Internet Explorer and go to <http://www.eicar.org>



Select "Anti-Malware Testfile"

Try downloading "eicar.com", "eicar.com.txt", "eicar.com.zip", "eicarcom2.zip". You can also test the SSL enabled downloads. The AV software should block them all. (You may have to add the eicar site to the trusted sites list to carry out this test.)

Trend Micro OfficeScan Resource Usage

Disk Space usage:

D drive: 171 MB

Process	Description	Typical Virtual Memory usage during normal CallPilot operation	Maximum Virtual Memory usage observed
AosUImanager.exe	Add-on Service Client User Interface		
CNTAoSMgr.exe	Add-on Service Client Management Service	1.1 MB	1.9 MB
CNTAoSUnInstaller.exe	Add-on Service Client Uninstaller		
INSTREG.exe			
LogServer.exe	Log Service		
ncfg.exe	Common Firewall Installer		
NTRmv.exe	Common Client Uninstallation Service		
NTRtScan.exe	Real-time Scan Service	27.2 MB	35.6 MB
OfcPfwSvc.exe			
PATCH.exe	Patch Program		
PccNT.exe	Management Console	2.8 MB	3 MB
PccNTMon.exe	Monitor	4.2 MB	6.1 MB
PccNTUpd.exe	Process Management Service		
SurrogateTmListen.exe	Surrogate Communication Service		
tdiins.exe	TMtdi Installer		
TMBMSRV.exe	Manages unauthorized change prevention feature		
TmFpHcEx.exe	NSC FPHC Extension		
TmListen.exe	Communication Service	13.4 MB	56.4 MB
tmlwfins.exe	NDIS 6.0 Filter Driver Installation Module		
TmNTUpgd.exe	CNTTmNTUpgd Application		
TmPfw.exe	Personal Firewall		
TmProxy.exe	Proxy Service		
TmUninst.exe			
tmwfpins.exe	WFP callout Driver Installation Module		
TSC.exe	Damage Cleanup Engine	0 MB	11.9 MB
UpdGuide.exe			
Upgrade.exe	Upgrade Service		
VSEncode.exe			
XPUpg.exe	Multi-session Process Management Service		

OfficeScan processes run at normal priority (priority base = 8).

<End of Bulletin>

©2011 Avaya Inc. All rights reserved.

Avaya and the Avaya logo are trademarks of Avaya Inc. and are registered in the United States and other countries.

All trademarks identified by ©, TM, or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc.

All other trademarks are the property of their respective owners. Avaya may also have trademark rights in other terms used herein.

The information in this document is subject to change without notice. Avaya reserves the right to make changes, without notice, in equipment design as engineering or manufacturing methods may warrant. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Avaya.