Antivirus Software Review (part 1)

Company	Product
ClamXAV	ClamXav.org?
Symantec	Norton Anti-Virus 9.0.2
Sophos	Anti-Virus 3.8.7
Intego	VirusBarrier X 10.1.1
McAfee	Virex 7.5.1

Objective:

Specify Antivirus software for use in the College of Fine Arts.

Method:

Load AV software on Faculty/Staff image known to have PC virus'.

Document how AV software performs with respect to;

1. Ease of software installation
2. Ease and method of applying virus definitions
3. Ability to detect existing virus'
4. Options for handling (eradicate, repair etc.) virus'
5. Ability to detect email (mbox) virus'
6. Options for handling Microsoft (Macro) virus'
7. User interface
8. Scan speed and overhead

Faculty Staff Image

Created separate partition for each antivirus app.

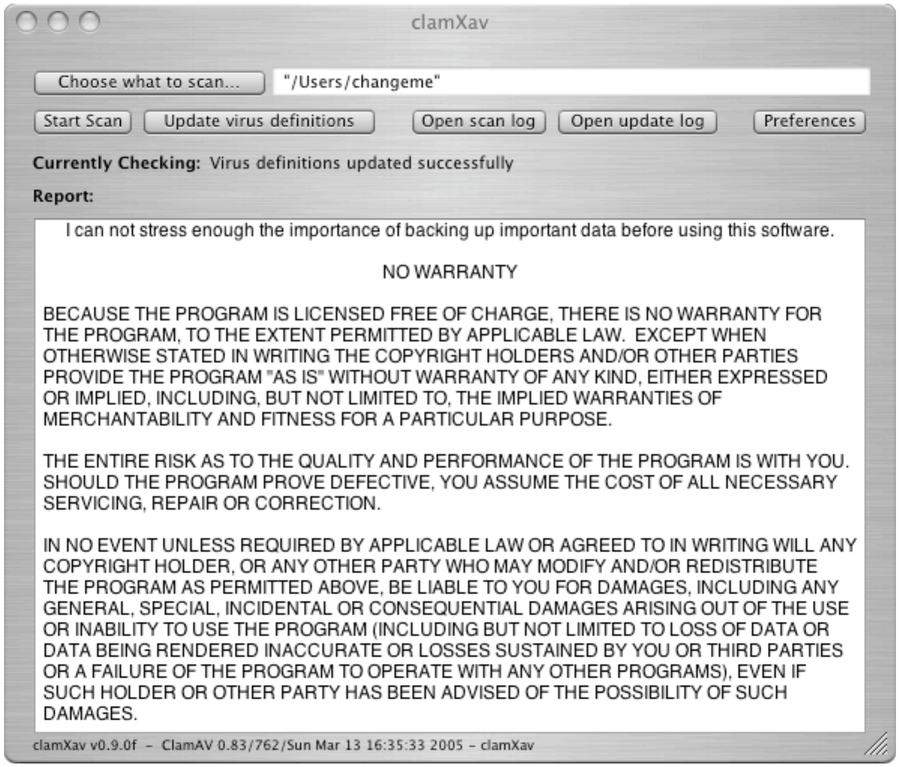
OS 10.3.8 with all standard Apple apps,
Microsoft Office 2004,
Eudora, Mail and Entourage

Loaded known PC viruses in

- ~Documents
- Mail mboxes
- Entourage mboxes

ClamAV

www.clamav.net



"/Users/changeme"

Currently Checking: Virus definitions updated successfully

Report:

I can not stress enough the importance of backing up important data before using this software.

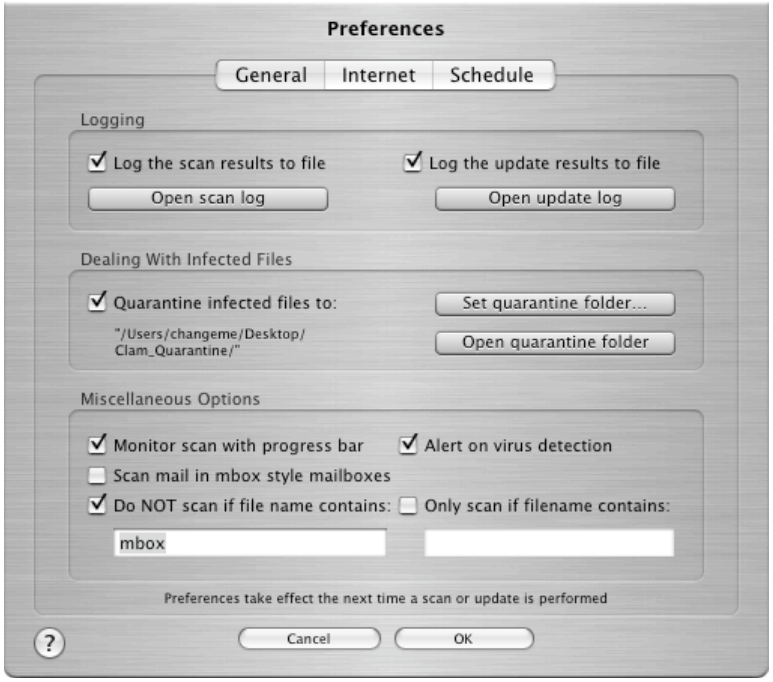
NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

clamXav v0.9.0f – ClamAV 0.83/762/Sun Mar 13 16:35:33 2005 – clamXav



Logging

☑ Log the scan results to file ☑ Log the update results to file

Dealing With Infected Files

☑ Quarantine infected files to:

"/Users/changeme/Desktop/
Clam_Quarantine/"

Miscellaneous Options

☑ Monitor scan with progress bar ☑ Alert on virus detection

□ Scan mail in mbox style mailboxes

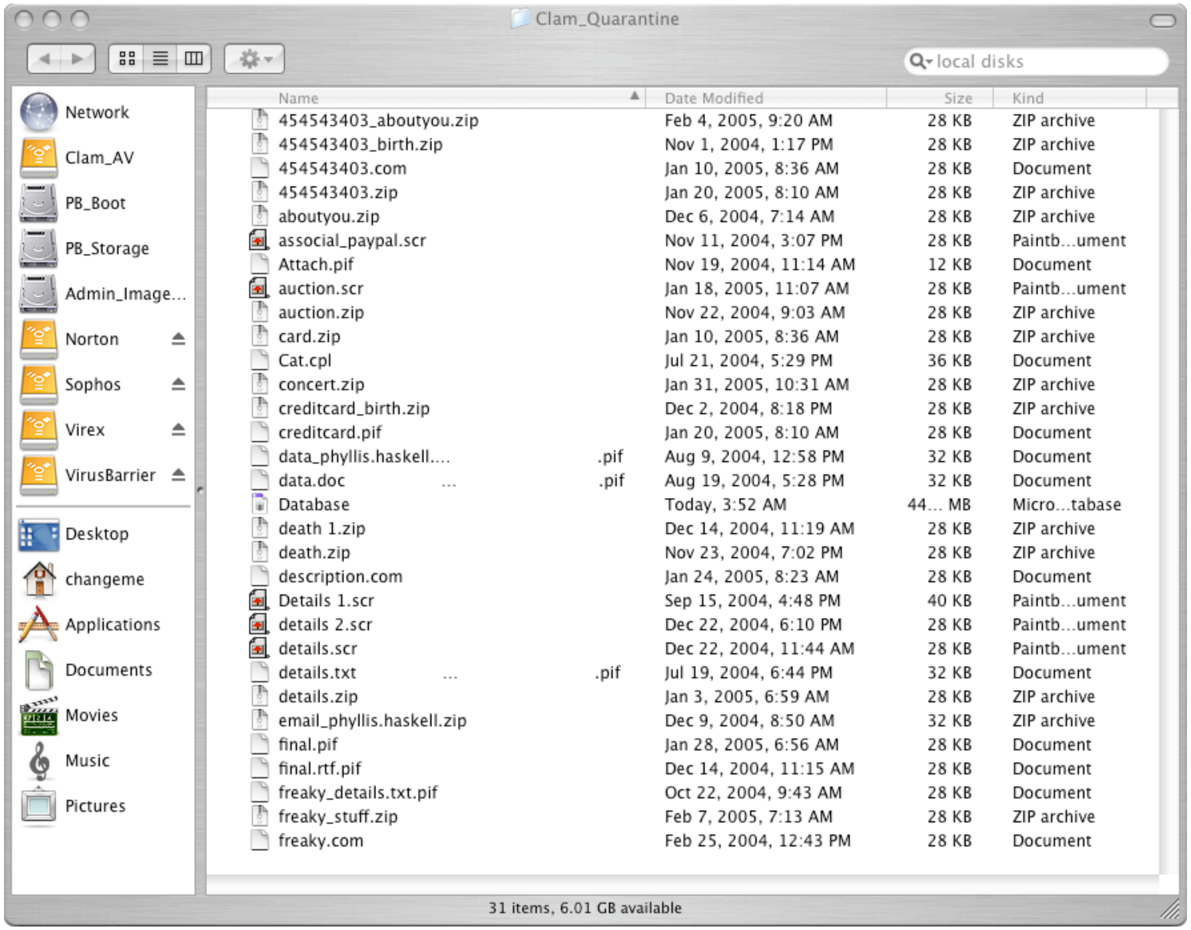
☑ Do NOT scan if file name contains: □ Only scan if filename contains:

mbox

Preferences take effect the next time a scan or update is performed

ClamAV

www.clamav.net



Name	Date Modified	Size	Kind
454543403_aboutyou.zip	Feb 4, 2005, 9:20 AM	28 KB	ZIP archive
454543403_birth.zip	Nov 1, 2004, 1:17 PM	28 KB	ZIP archive
454543403.com	Jan 10, 2005, 8:36 AM	28 KB	Document
454543403.zip	Jan 20, 2005, 8:10 AM	28 KB	ZIP archive
aboutyou.zip	Dec 6, 2004, 7:14 AM	28 KB	ZIP archive
associal_paypal.scr	Nov 11, 2004, 3:07 PM	28 KB	Paintb...ument
Attach.pif	Nov 19, 2004, 11:14 AM	12 KB	Document
auction.scr	Jan 18, 2005, 11:07 AM	28 KB	Paintb...ument
auction.zip	Nov 22, 2004, 9:03 AM	28 KB	ZIP archive
card.zip	Jan 10, 2005, 8:36 AM	28 KB	ZIP archive
Cat.cpl	Jul 21, 2004, 5:29 PM	36 KB	Document
concert.zip	Jan 31, 2005, 10:31 AM	28 KB	ZIP archive
creditcard_birth.zip	Dec 2, 2004, 8:18 PM	28 KB	ZIP archive
creditcard.pif	Jan 20, 2005, 8:10 AM	28 KB	Document
data_phyllis.haskell.... .pif	Aug 9, 2004, 12:58 PM	32 KB	Document
data.doc ... .pif	Aug 19, 2004, 5:28 PM	32 KB	Document
Database	Today, 3:52 AM	44... MB	Micro...tabase
death 1.zip	Dec 14, 2004, 11:19 AM	28 KB	ZIP archive
death.zip	Nov 23, 2004, 7:02 PM	28 KB	ZIP archive
description.com	Jan 24, 2005, 8:23 AM	28 KB	Document
Details 1.scr	Sep 15, 2004, 4:48 PM	40 KB	Paintb...ument
details 2.scr	Dec 22, 2004, 6:10 PM	28 KB	Paintb...ument
details.scr	Dec 22, 2004, 11:44 AM	28 KB	Paintb...ument
details.txt ... .pif	Jul 19, 2004, 6:44 PM	32 KB	Document
details.zip	Jan 3, 2005, 6:59 AM	28 KB	ZIP archive
email_phyllis.haskell.zip	Dec 9, 2004, 8:50 AM	32 KB	ZIP archive
final.pif	Jan 28, 2005, 6:56 AM	28 KB	Document
final.rtf.pif	Dec 14, 2004, 11:15 AM	28 KB	Document
freaky_details.txt.pif	Oct 22, 2004, 9:43 AM	28 KB	Document
freaky_stuff.zip	Feb 7, 2005, 7:13 AM	28 KB	ZIP archive
freaky.com	Feb 25, 2004, 12:43 PM	28 KB	Document

31 items, 6.01 GB available

ClamAV

www.clamav.net

Ease of software installation	Installer, then drag app
Ease and method of applying virus definitions	Manual or schedule (Admin)
Ability to detect existing viruses	Found 12, moved 6, moved more each run
Options for handling (eradicate, repair etc.) virus'	No repair
Ability to detect email (mbox) virus'	Poor, breaks them
Options for handling Microsoft (Macro) virus'	None
User interface	GUI is OK for free
On Access Scanner	None but has scheduler Admin issue
Scan speed and overhead (/Users folder)	1st run :53, 2nd run 1:21

ClamAV notes

- •Open source
- •Nice interface
- •Defs provided by open source community
- •Can trash mbox style mailboxes
- •Can trash Entourage database

Norton Anti-virus

Demo

Norton Anti-virus 9.0.2

www.symantec.com

Ease of software installation	.pkg installer, reboot
Ease and method of applying virus definitions	Slow?, annoying window
Ability to detect existing virus’	Found 126
Options for handling (eradicate, repair etc.) virus’	Configurable
Ability to detect email (mbox) virus’	Missed them
Options for handling Microsoft (Macro) virus’	Did not test
User interface	Obtrusive
On Access Scanner	On Mount
Scan speed and overhead	1st run 7:00 2nd run :01

Norton Anti-virus notes

- Runs fast
- Granular control of what to scan
- Schedule updates and scans
- On-Access scan?
- Annoying interface

Sophos Anti-Virus

Demo

Sophos Anti-Virus 3.8.7

www.sophos.com

Ease of software installation	.pkg and reboot
Ease and method of applying virus definitions	*config. to your server
Ability to detect existing viruses	1st 120, 233 after 2
Options for handling (eradicate, repair etc.) viruses	Configurable
Ability to detect email (mbox) viruses	Error
Options for handling Microsoft (Macro) viruses	Seems to clean them
User interface	Fair
On Access Scanner	Works great!
Scan speed and overhead	1st immed run apx 1 hr. 50 - 70% cpu 2nd immed. Run 1:05 50 - 70% cpu **On Access scanner low overhead**

Sophos Anti-Virus Notes

- Able to send email notification
- On-access scanner works great with low overhead
- How does it handle mbox mailboxes?

Antivirus Software Review (part 2)

Company	Product
Intego	VirusBarrier X 10.1.1
McAfee	Virex 7.5.1
Sophos	Win2k server & client management

VirusBarrier 1.6.2

Demo

VirusBarrier 1.6.2

www.intego.com

Ease of software installation	Fair
Ease and method of applying virus definitions	OK reboot?
Ability to detect existing viruses	Only in your user folder
Options for handling (eradicate, repair etc.) viruses	Scan, Repair
Ability to detect email (mbox) viruses	? App kept quitting
Options for handling Microsoft (Macro) viruses	Claims to fix
User interface	Fair
On Access Scanner	Claims to have
Scan speed and overhead	26 min* 70% in top (*found nothing)

VirusBarrier 1.6.2 Notes

- Got best review from Macworld
- Documentation has good virus info
- Reboot required after install and update
- Repair of volume as admin did nothing
- Can not scan other User folders
- Scan Email Attachments quit app
- Log never showed anything

Virex 7.5.1

Demo

Virex 7.5.1

www.mcafee.com

Ease of software installation	Good
Ease and method of applying virus definitions	Good
Ability to detect existing viruses	Found 127
Options for handling (eradicate, repair etc.) viruses	No Repair
Ability to detect email (mbox) viruses	No
Options for handling Microsoft (Macro) viruses	?
User interface	Limited
On Access Scanner	New in 7.?
Scan speed and overhead	2.5 hr (volume) 70% in top Virex 30% for Virex Vshield

Virex 7.5.1 Notes

- At $5.00 it is the cheapest
- 7.5.1 is much improved, better logging and on access features added
- Rescan does not get faster
- Clean = Delete
- Move to trash = Delete
- Heavy overhead at 30 - 50% running in background

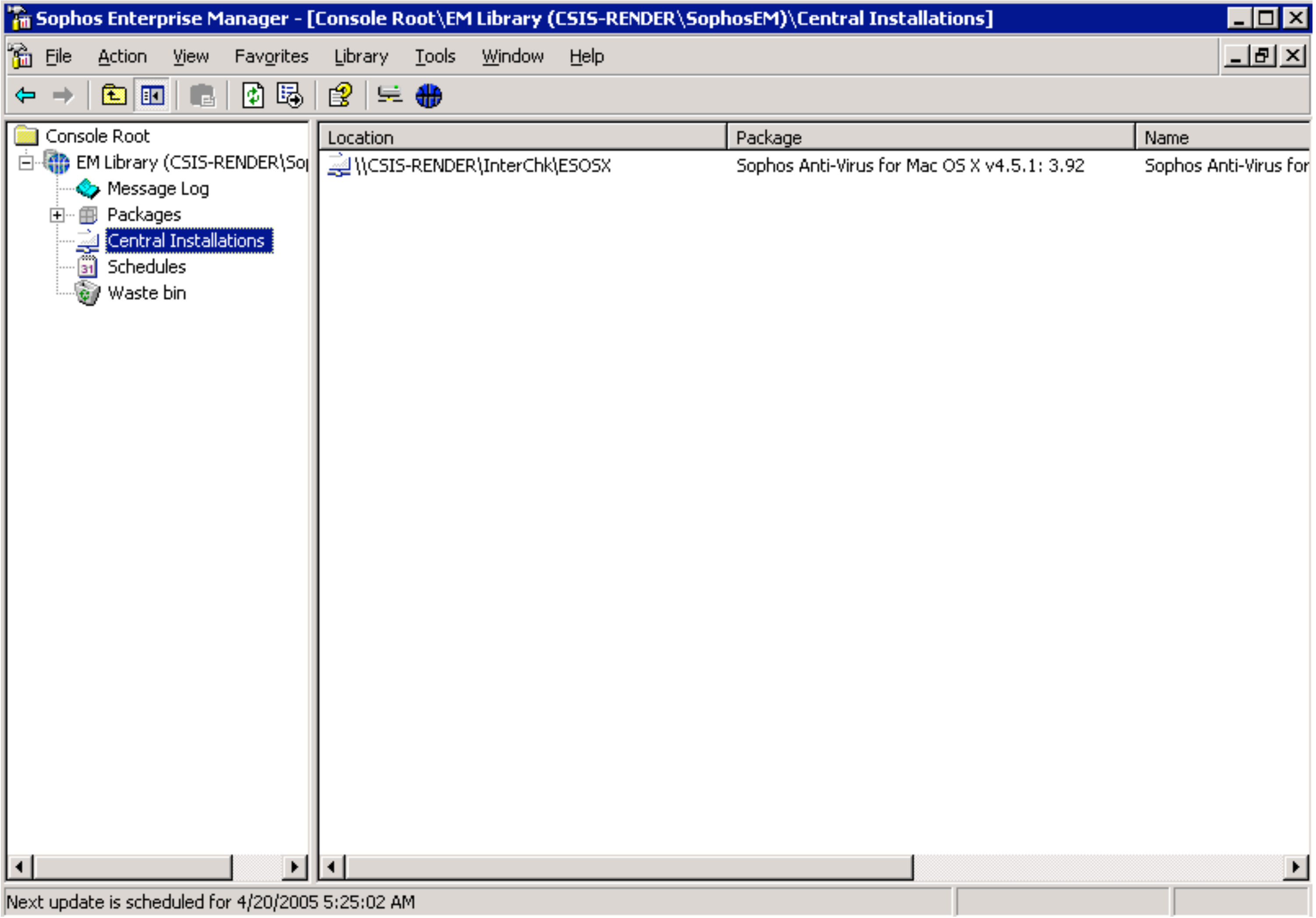
Results

Test	ClamAV	Norton	Sophos	VB	Virex
Price	Free	$19	$25 (100, 3yr)	$36? (10, 1yr)	$5
Ease of software installation	Good	Good	Good	Good	Good
Ease and method of applying virus definitions	Good	Good	Fair	Fair	Good
Ability to detect existing viruses	Found 31	Found 126	Found 120/233	App Quit	Found 127
Options for handling (eradicate, repair etc.) viruses	No repair	Can Config.	Can Config.	Scan repair	No Repair
Ability to detect email (mbox) viruses	No	?	Error	App Quit	No
Options for handling Microsoft (Macro) viruses	No	?	Yes	Claims	Claims
User interface	Fair	Fair	Fair	Fair	Limited
On-Access Scan	None	Good	Good	Claims	Good
Scan speed and overhead	:53/1:21	7/:01	(Volume) 1:00	(Volume) :26	(Volume) 2:30

Conclusions

- I would rate
- 1 Sophos
- 2 Norton
- 3 Virex
- All have on-access scanners
- All 3 found ~120 viruses
- Only Sophos has the ability to notify

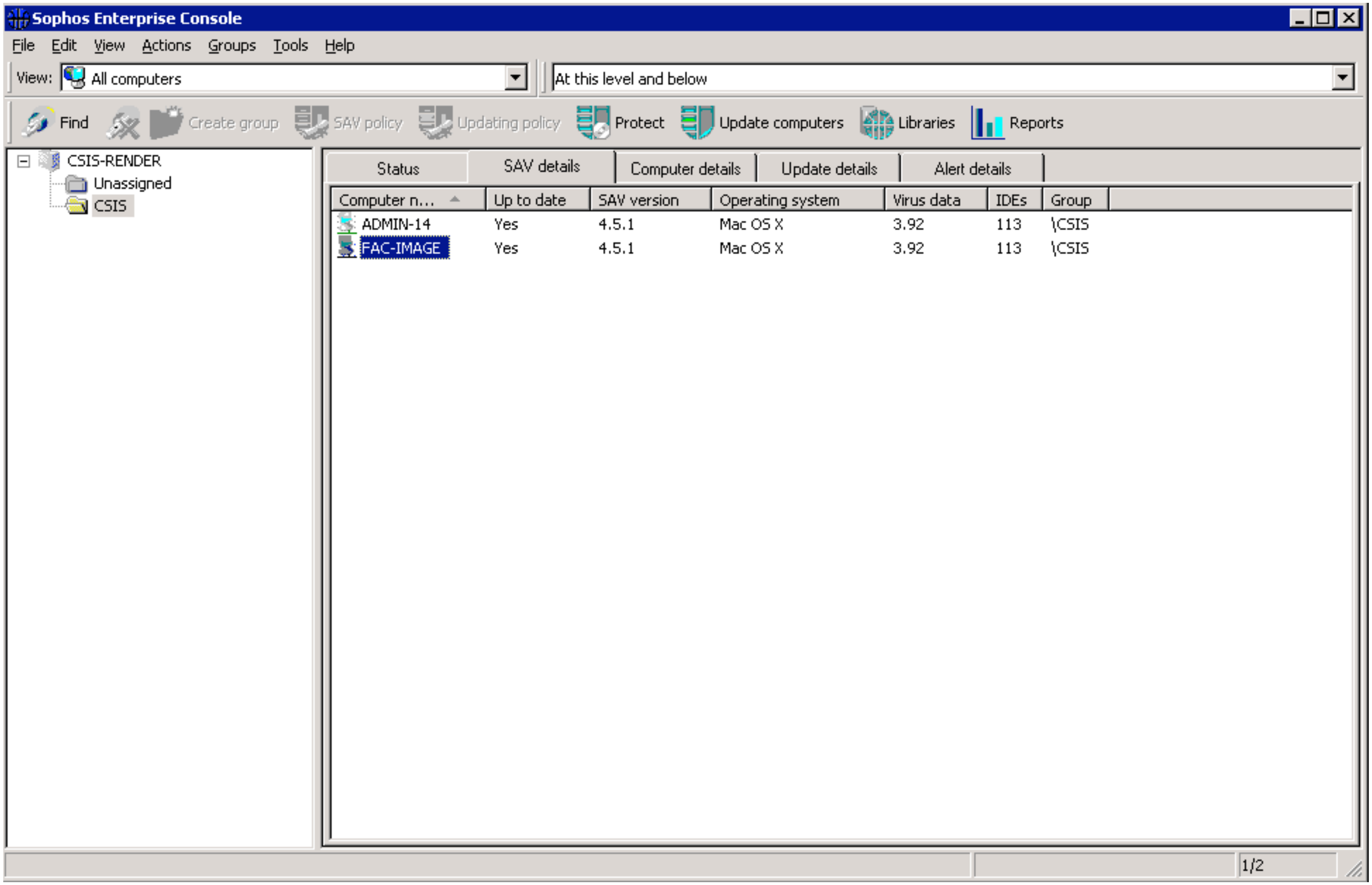
Sophos Enterprise Manager 2.0 v5.2


Sophos Enterprise Manager - [Console Root\EM Library (CSIS-RENDER\SophosEM)\Central Installations]
File
Action
View
Favorites
Library
Tools
Window
Help
Console Root
EM Library (CSIS-RENDER\So|
Message Log
Packages
Central Installations
Schedules
Waste bin

Location	Package	Name
\\CSIS-RENDER\InterChk\ESOSX	Sophos Anti-Virus for Mac OS X v4.5.1: 3.92	Sophos Anti-Virus for

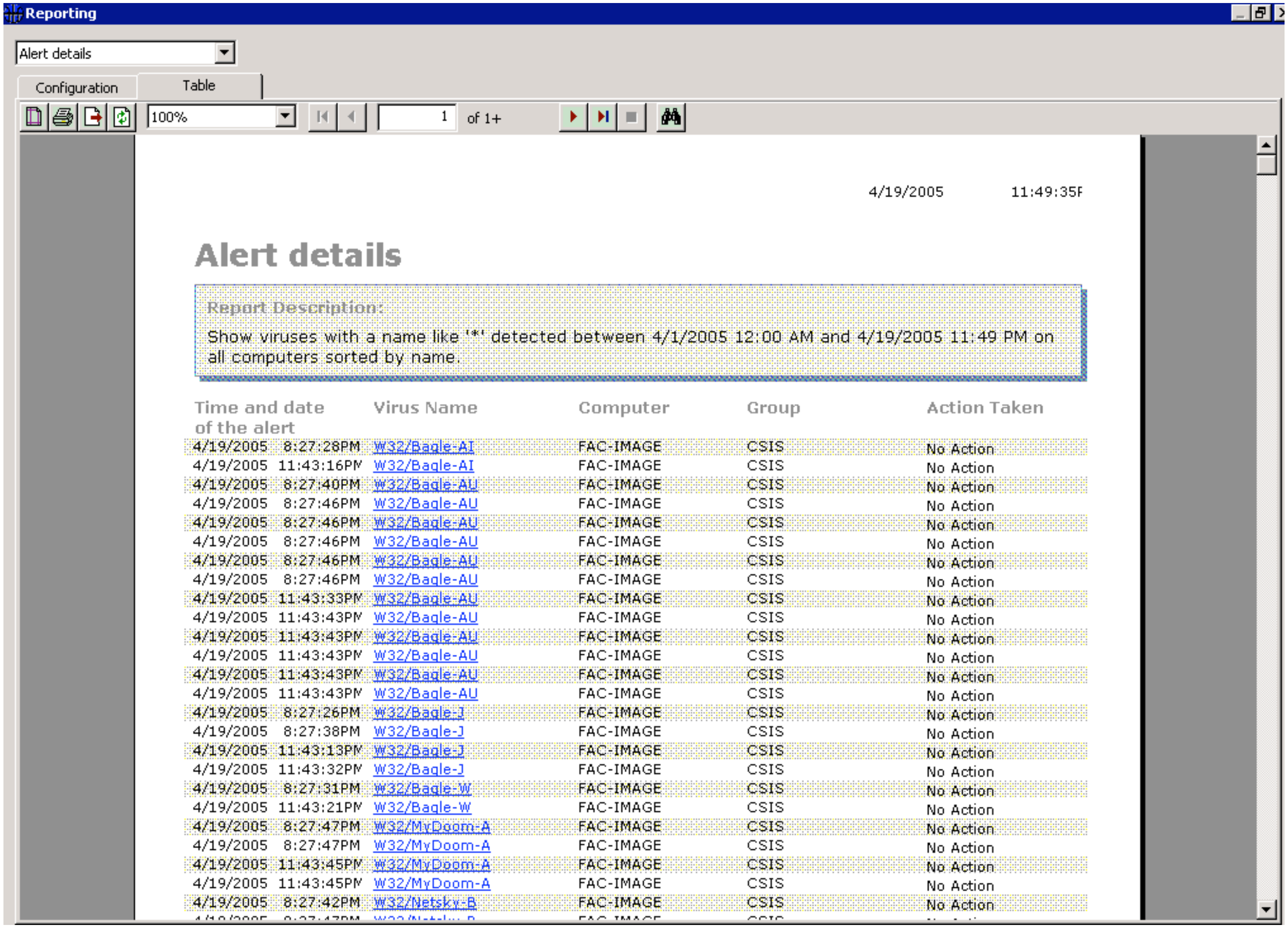
Next update is scheduled for 4/20/2005 5:25:02 AM

Sophos Enterprise Console 1.0



Computer n...	Up to date	SAV version	Operating system	Virus data	IDEs	Group
ADMIN-14	Yes	4.5.1	Mac OS X	3.92	113	\CSIS
FAC-IMAGE	Yes	4.5.1	Mac OS X	3.92	113	\CSIS

Sophos Enterprise Console
Alert Details Report



4/19/2005 11:49:35P

Alert details

Report Description:

Show viruses with a name like '*' detected between 4/1/2005 12:00 AM and 4/19/2005 11:49 PM on all computers sorted by name.

Time and date of the alert	Virus Name	Computer	Group	Action Taken
4/19/2005 8:27:28PM	W32/Bagle-AI	FAC-IMAGE	CSIS	No Action
4/19/2005 11:43:16PM	W32/Bagle-AI	FAC-IMAGE	CSIS	No Action
4/19/2005 8:27:40PM	W32/Bagle-AU	FAC-IMAGE	CSIS	No Action
4/19/2005 8:27:46PM	W32/Bagle-AU	FAC-IMAGE	CSIS	No Action
4/19/2005 8:27:46PM	W32/Bagle-AU	FAC-IMAGE	CSIS	No Action
4/19/2005 8:27:46PM	W32/Bagle-AU	FAC-IMAGE	CSIS	No Action
4/19/2005 8:27:46PM	W32/Bagle-AU	FAC-IMAGE	CSIS	No Action
4/19/2005 8:27:46PM	W32/Bagle-AU	FAC-IMAGE	CSIS	No Action
4/19/2005 11:43:33PM	W32/Bagle-AU	FAC-IMAGE	CSIS	No Action
4/19/2005 11:43:43PM	W32/Bagle-AU	FAC-IMAGE	CSIS	No Action
4/19/2005 11:43:43PM	W32/Bagle-AU	FAC-IMAGE	CSIS	No Action
4/19/2005 11:43:43PM	W32/Bagle-AU	FAC-IMAGE	CSIS	No Action
4/19/2005 11:43:43PM	W32/Bagle-AU	FAC-IMAGE	CSIS	No Action
4/19/2005 11:43:43PM	W32/Bagle-AU	FAC-IMAGE	CSIS	No Action
4/19/2005 8:27:26PM	W32/Bagle-J	FAC-IMAGE	CSIS	No Action
4/19/2005 8:27:38PM	W32/Bagle-J	FAC-IMAGE	CSIS	No Action
4/19/2005 11:43:13PM	W32/Bagle-J	FAC-IMAGE	CSIS	No Action
4/19/2005 11:43:32PM	W32/Bagle-J	FAC-IMAGE	CSIS	No Action
4/19/2005 8:27:31PM	W32/Bagle-W	FAC-IMAGE	CSIS	No Action
4/19/2005 11:43:21PM	W32/Bagle-W	FAC-IMAGE	CSIS	No Action
4/19/2005 8:27:47PM	W32/MyDoom-A	FAC-IMAGE	CSIS	No Action
4/19/2005 8:27:47PM	W32/MyDoom-A	FAC-IMAGE	CSIS	No Action
4/19/2005 11:43:45PM	W32/MyDoom-A	FAC-IMAGE	CSIS	No Action
4/19/2005 11:43:45PM	W32/MyDoom-A	FAC-IMAGE	CSIS	No Action
4/19/2005 8:27:42PM	W32/Netsky-B	FAC-IMAGE	CSIS	No Action

?