

Instructions for Installing and Configuring ClamXav Antivirus Software for Macs

Towson University

Computers that are on the Internet share files and e-mail and are vulnerable to viruses, spyware, and malware. Macs are less susceptible to viruses than Windows computers but can pass viruses on to other users if you do not install antivirus software that scans and cleans viruses.

Protect your computer and prevent the spread of viruses with ClamXav, a free virus scanner for Macs that can detect and remove both Windows and Mac threats. Follow the instructions below to install ClamXav.

ClamXav Installation and Configuration Instructions

Below are the recommended settings for faculty, staff, and students. Information for classroom and computer labs is available in section E.

Only one antivirus program should be installed on a computer. If you already have another antivirus application installed on your Mac, the first step is to uninstall (remove) that application before installing ClamXav. Below are instructions for uninstalling McAfee VirusScan on-campus and off campus. If you have antivirus software, check with the software vender for instructions on how to uninstall it. If you do not have antivirus software installed, proceed to section B. to install ClamXav.

A. Remove McAfee VirusScan

Instructions For Removing VirusScan On-Campus

Macs that are on campus and plugged into the network can follow these instructions.

1. In Finder, Click “Go” and then select “Connect to Server” (Fig. 1)
2. In the Server Address field (Fig. 2) type:
smb://customshare/MacSoftware/McAfee
3. Click “Connect”
4. A file directory will open, double-click the file: “VirusScanMac8.6.1.dmg”



Figure 1

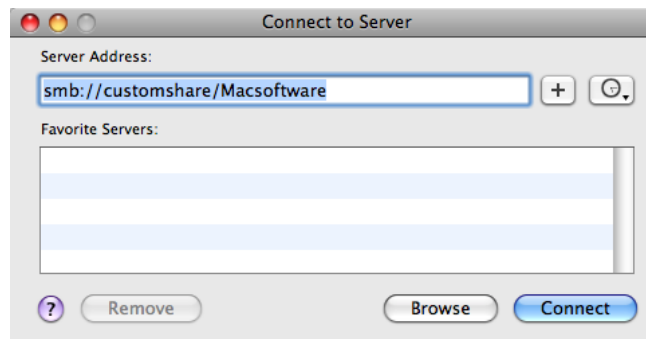


Figure 2

In the VirusScanForMac 8.6.1 window, copy the “VirusScan Uninstall.command” file to your Mac desktop (Fig. 3)

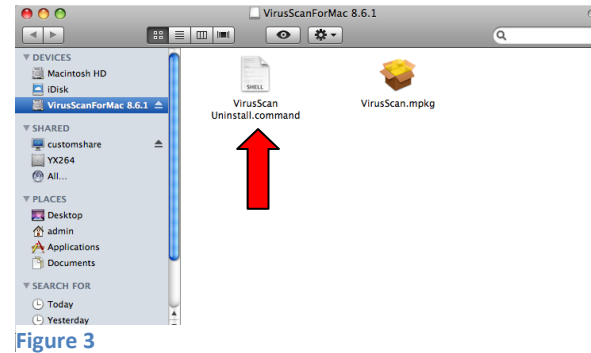


Figure 3

5. On your Desktop, double-click on the “VirusScan Uninstall.command” file, a Terminal window will appear and request a password (Fig. 4).
6. Type your User password, press “Enter” and wait for the terminal window to tell you the process is complete. This will uninstall McAfee VirusScan.
Note : user must have administrator rights to uninstall VirusScan

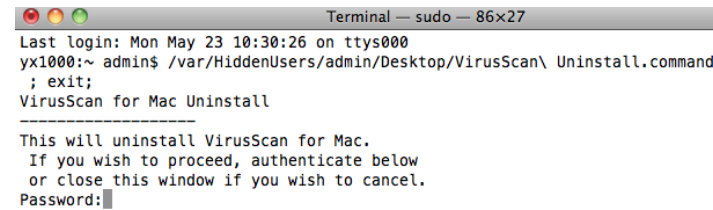


Figure 4

Occasionally, you may have to restart the Mac and repeat the steps above to remove VirusScan. If VirusScan will not remove, follow the Off-Campus instructions below.

Instructions For Removing VirusScan Off-Campus

To remove McAfee from Macs off-campus or if the on-campus procedures above fail to remove McAfee, select [this link](#) for instructions.

B. Install ClamXav

Requirements: You must logon with administrator rights to install ClamXav on the Mac.

1. Download ClamXav from <http://www.clamxav.com/>
2. **Drag** the ClamXav.app icon into the Applications folder (Fig. 5)

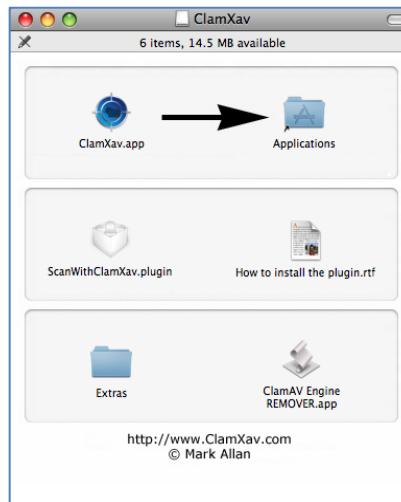


Figure 5

3. In Applications, double click ClamXav.app
4. You will be prompted to install the Clam Anti-Virus engine (Fig. 6)

Click "Install" and follow the onscreen instructions. Once the installer has finished, double click ClamXav.app again

When prompted for a location in the Select a Destination window, select "Macintosh hard drive"

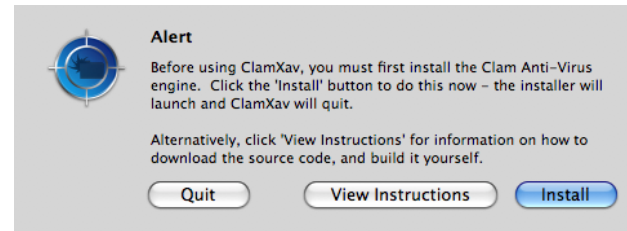


Figure 6

C. Configure ClamXav Preferences

1. Click the "Preferences" icon (Fig. 7)

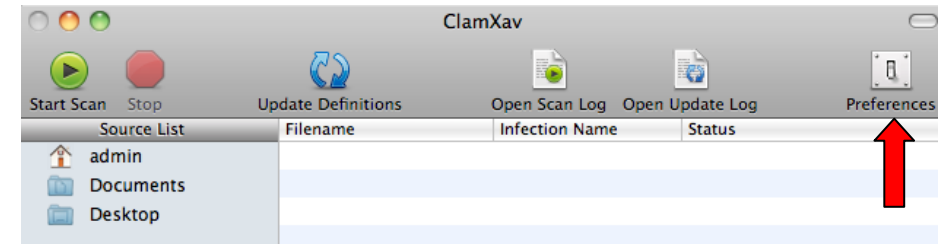


Figure 7

In the Preferences "General" tab, check all boxes exactly as seen in Fig. 8, do NOT check "Include anonymous system profile information", exactly

2. "Quarantine" tab: the recommendation is not to configure the Quarantine feature, ignore this setting

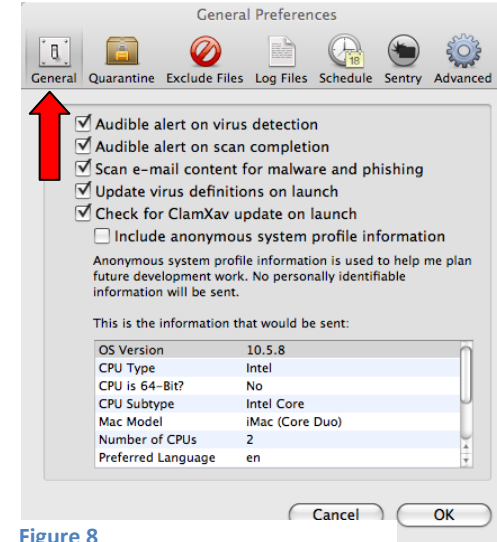


Figure 8

3. Select the Preferences “Schedule” tab for Schedule Preferences (Fig. 9)

4. Under “Update Virus Definitions” select “Every Day” on the drop down menu

Enter a time that the computer is powered on but will not interrupt your work

5. Under “Scan” (Fig. 9), select a day and time that the computer is powered on but will not interrupt your work; a scan can take several hours to complete; you can work on the Mac during a scan but should avoid performing intense processing operations such as 3-D modeling, or video and audio editing during a scheduled virus scan

6. Under “Scan” click the “+” button (Fig. 9)

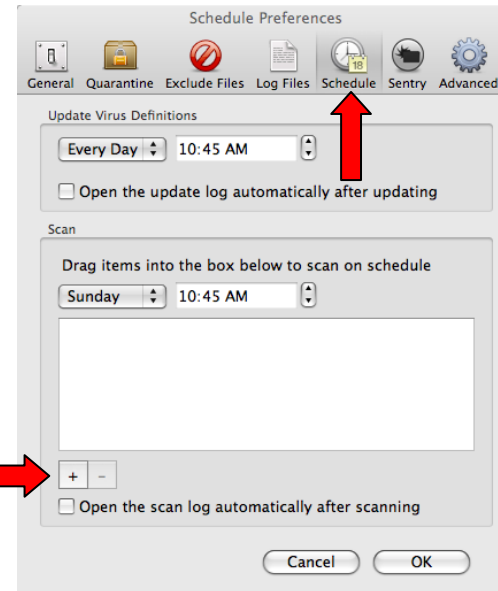


Figure 9

7. In the selection window (Fig. 10), select Macintosh (hard drive) and click “open”

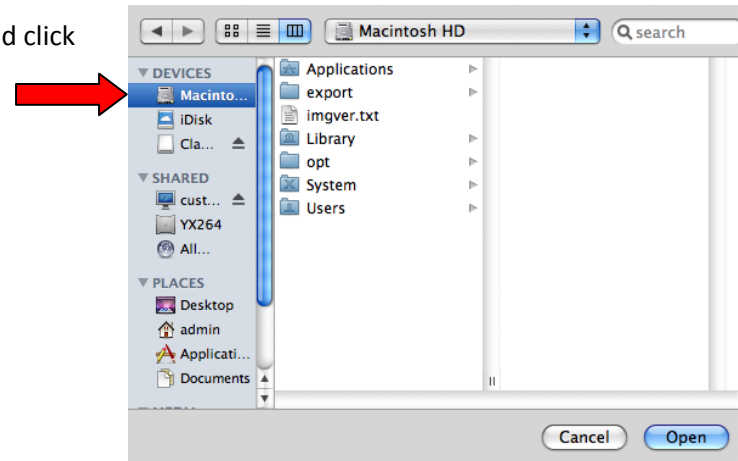


Figure 10

In The Scheduled Preferences window, the “/” that appears (highlighted in blue) represents the hard drive (Fig. 11)

8. Click “OK” (Fig. 11)

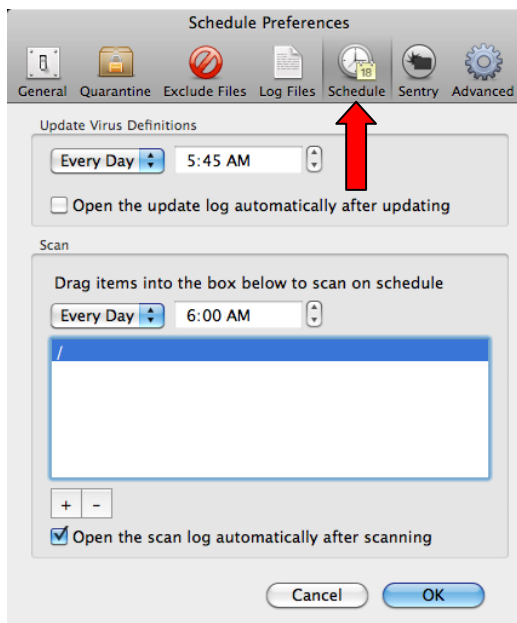


Figure 11

The Sentry preference settings are below. ClamXav Sentry launches when you logon to a Mac to monitor and protect it.

9. In the Preferences window, click the “Sentry” tab (Fig. 12)
10. In the ClamX Sentry Preferences window, click the “+” button

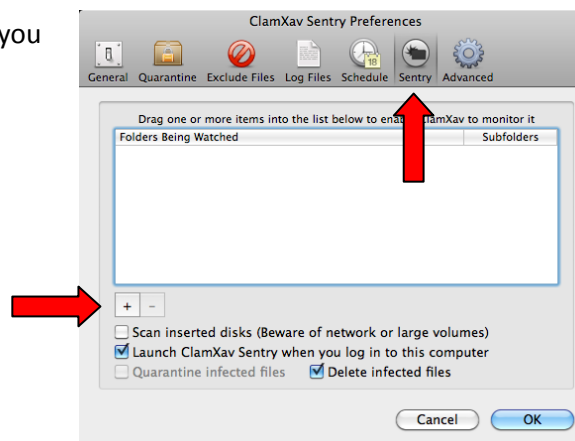


Figure 12

11. Choose Macintosh (hard drive) and click “open” (Fig. 13)

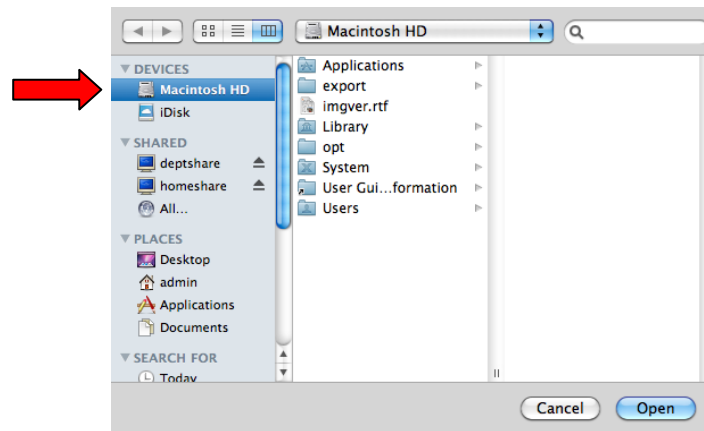


Figure 13

In the ClamXav Sentry Preferences window: (Fig. 14)

12. Check the Subfolders box

13. Check the box to “Launch ClamXav Sentry when you log in to this computer”

14. Check the box to “Delete infected files”;

Sentry preferences should be set exactly as seen in Fig. 14

15. Click “OK” (Fig. 14)

ClamXav is now installed and configured only for the user that is logged on.

D. For Computers Shared by Multiple Users

IMPORTANT: If the Mac is shared with other users, each user that shares the Mac will need to configure ClamXav Preferences to enable protection when they log on to the computer. Follow these instructions:

1. Log on to the Mac
2. Go to “Applications” and open ClamXav
3. Follow the instructions above in section: “Configure ClamXav Preferences”

E. For University Classroom and Computer Labs

The standard university configuration is available as an image that can be adapted for department classrooms and labs. This configuration is setup so that all users that logon to the Mac will automatically be protected and not have to configure ClamXav preferences. Contact Jack Stark if you are interested in the image or how the image was setup.

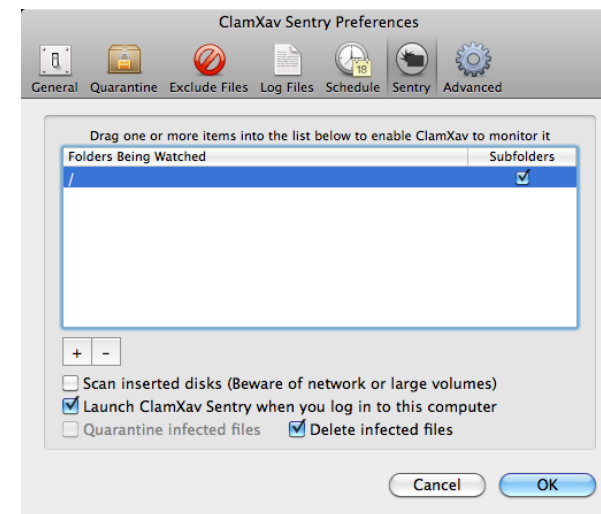


Figure 14

F. ClamXav Resources

- ClamXav site: <http://www.clamxav.com/index.php>
- ClamXav Preference Settings Details: http://www.clamxav.com/docs_prefs_general.php