

ClamXav

a free antivirus application for the Mac

Background

Why anti-virus software for Mac OS X, which has been virus-free for years?

- Viruses for OS X will eventually appear.
- You presumably don't want to pass on Windows viruses to your PC friends (they have enough virus trouble already).

The two functions of antivirus software:

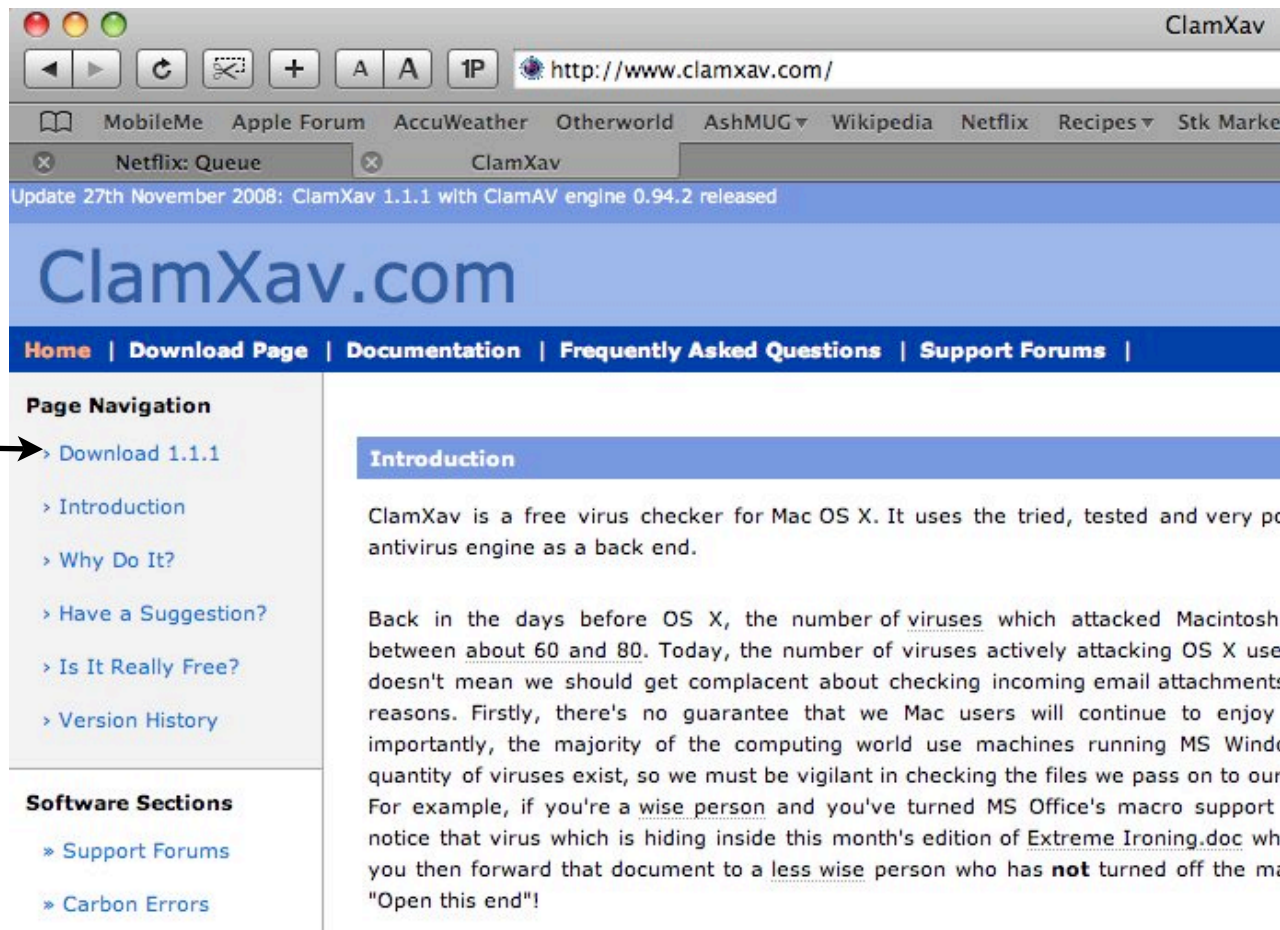
Prevent viruses from getting into your computer. (*The most important function*)
*In ClamXav this is called **Folder Sentry***

Find and eliminate any that are already on your machine.
*In ClamXav this is called **Scan***

I include *worms* and *trojans* under the term *virus*. For more information on the distinctions see <http://us.trendmicro.com/us/support/virus-primer/index.html>

Downloading and Installing

Go to the website www.clamxav.com



Select the version for your OS and click to download

ClamXav 1.1.1 with ClamAV 0.94.2 backend - 27th November 2008

Please choose the correct download for your version of Mac OS X.

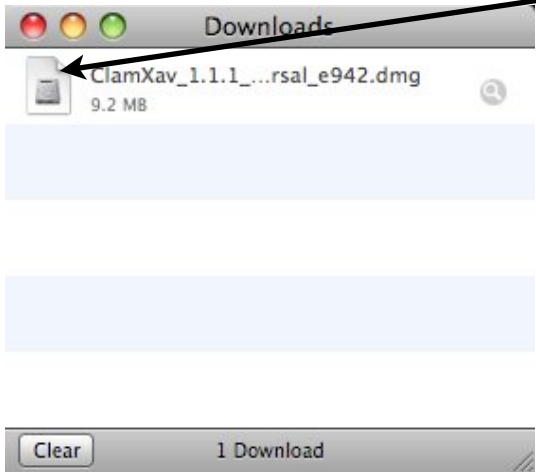
Download for 10.4 Tiger and 10.5 Leopard (preferred) | mirror (24.4 MB)

ClamXav is fully Universal which means that it will run on 10.4 and 10.5 on both PPC and

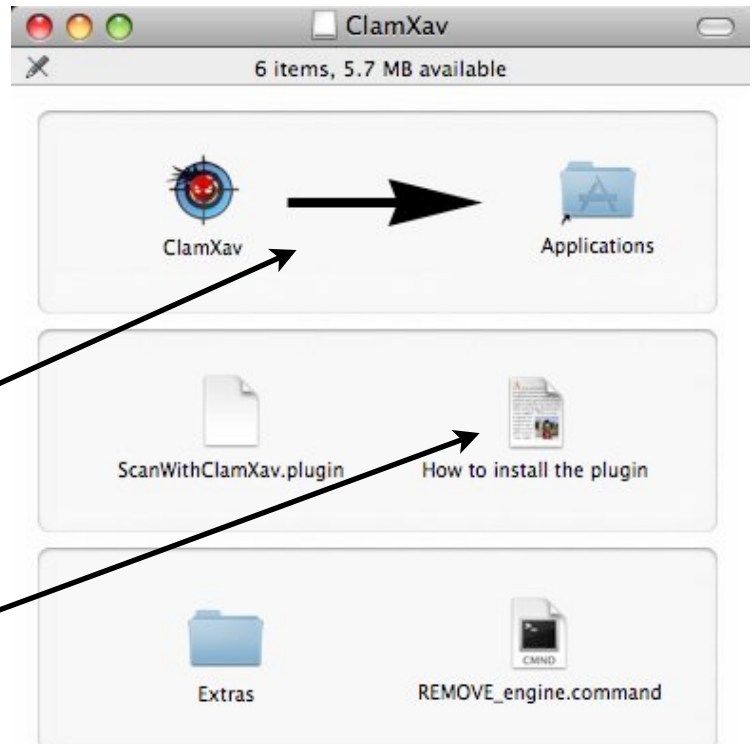
Download for 10.3 Panther | mirror (22.9 MB) - **Unsupported**

Please note: Since the release of Mac OS X 10.5, I no longer have the resources to m cease to operate correctly under Panther. For as long as my aging PowerBook continue: than that, I'm afraid I can't make any promises. Sorry.

When it is through downloading, double-click to mount the ClamXav installation disk image



If you don't see this small downloads window, you can go to your Downloads folder, desktop, or wherever you send your downloads and double click on it there.



The disk image will be mounted, and this window will be displayed.

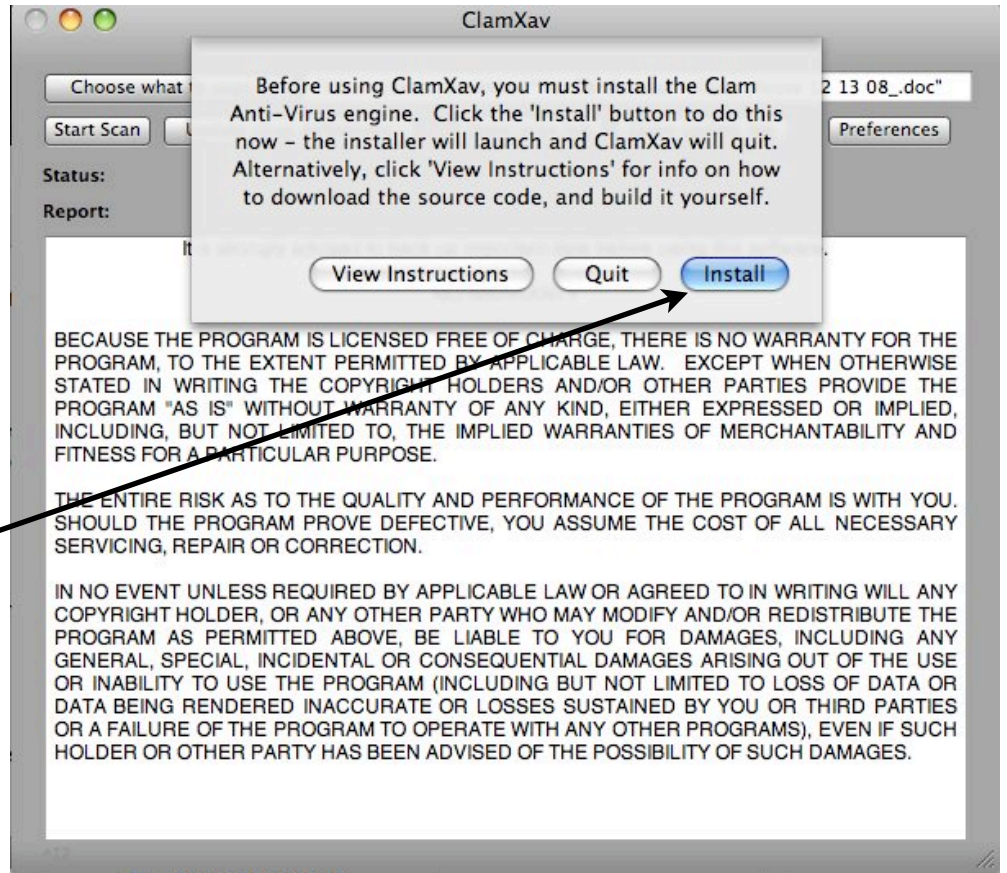
To install ClamXav, drag the icon as shown

To install the plug-in follow the instructions here

We've now installed ClamXav, but it is only the the user interface to the *scan engine*, which is what does all the work.

To install the scan engine, go to the applications folder and launch ClamXav.

Click here and you will be guided through the installation.

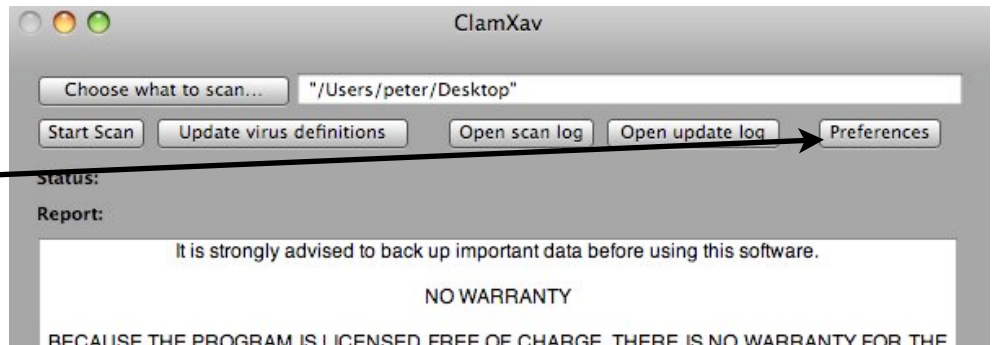


Folder Sentry

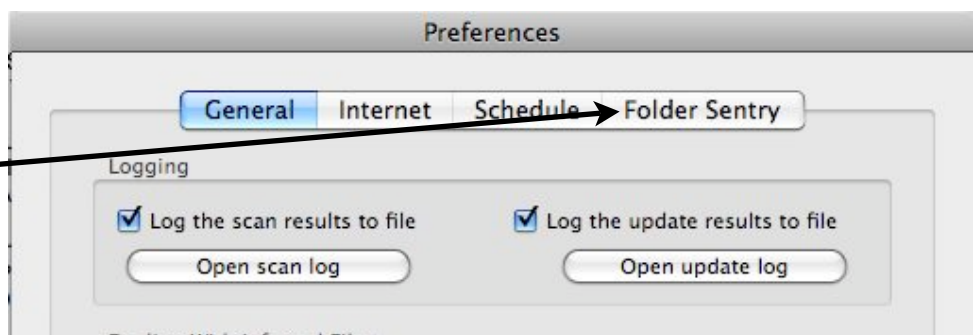
Note: The following discussions assume OS 10.5 and Apple Mail.

In my opinion the most important task is keeping viruses out of your computer, not finding them after they have already gotten in and you have forwarded the virus to someone else. Keeping them out is the job of Folder Sentry, and we will set this up first.

Open ClamXav and click on Preferences.

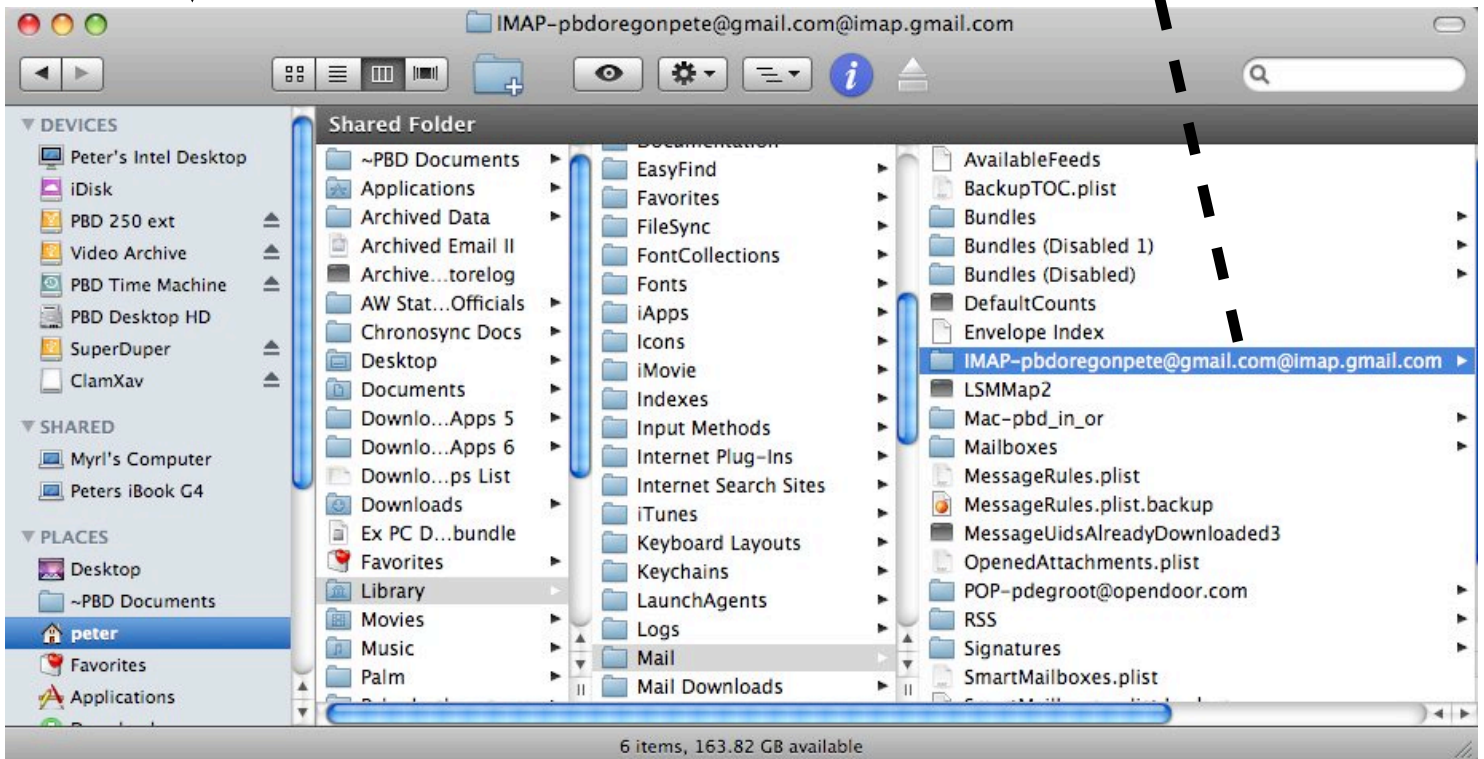
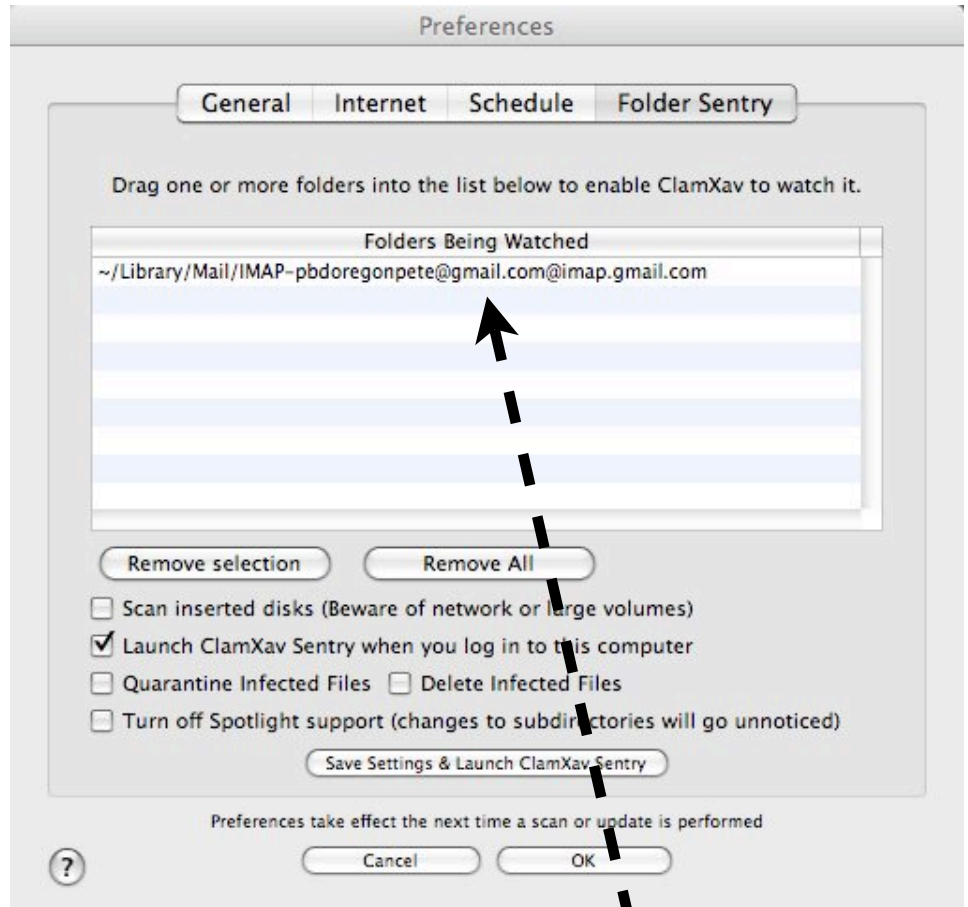


then click on Folder Sentry



This will open up a window where you can specify which folders you want Folder Sentry to watch.

Open a finder window, navigate to the folders you want, and drag them to the Folder Sentry window.



What folders should you have Folder Sentry watch?

At a minimum:

Your email Inbox or Inboxes if you have more than one account.

If you are using Apple Mail, these will be in *Home/Library/Mail*. They will be folders with POP or IMAP somewhere in the name. See the example on the previous page. Note that they are not in the folder named Mailboxes. These are mailboxes you have created "on my Mac". They don't have to be monitored because everything goes through the Inbox first.

Your Mail Downloads folder.

This is where email attachments are stored. By default it is *Home/Library/Mail Downloads* unless you have changed the folder for mail downloads in Mail/Preferences/General.

Your Downloads folder.

This is where your downloads from the internet end up. By default it is *Home/Downloads* unless you have changed it in your web browsers Preferences.

For many of us, this covers most of the ways that viruses can get in. Depending on how you use your computer, you may want to add some additional precautions. For example, if you

- Often get files on Flash drives, CDs, DVDs or portable Hard drives from other users.
- Often receive files via iChat
- Are running Windows on your Mac with a virtual machine via Boot Camp, Fusion, or Parallels

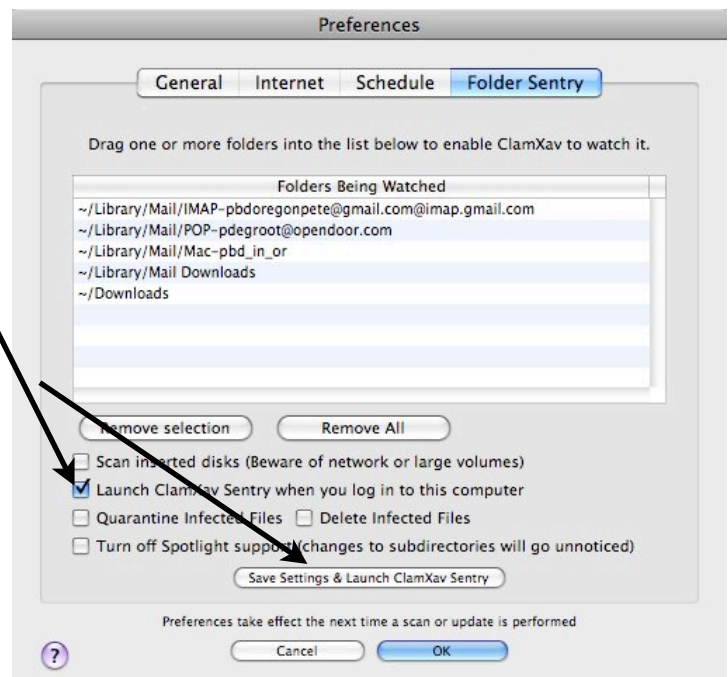
Some suggestions on dealing with these situations are given at the end of this document.

Start Folder Sentry's protection.

You want to check this box to have Folder Sentry start automatically when you log in.

Click this button to launch Folder Sentry. DON'T click the OK button.

If you click the OK button changes don't take place until after the next scan or update. If you use the Save Settings and Launch... button they take effect immediately, and it doesn't cause any problems if Folder Sentry is already running.



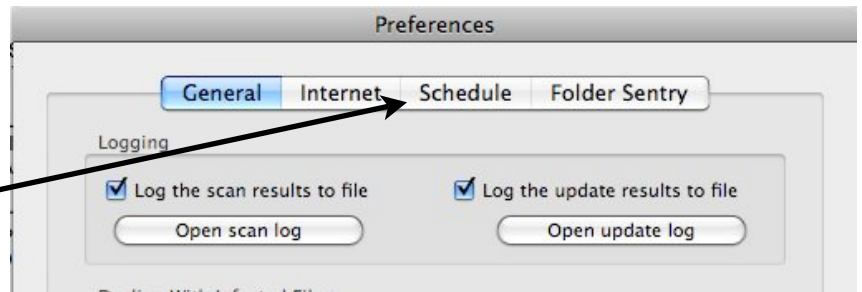
You should now see this icon  in the Menu Bar.

Updating Virus Definitions

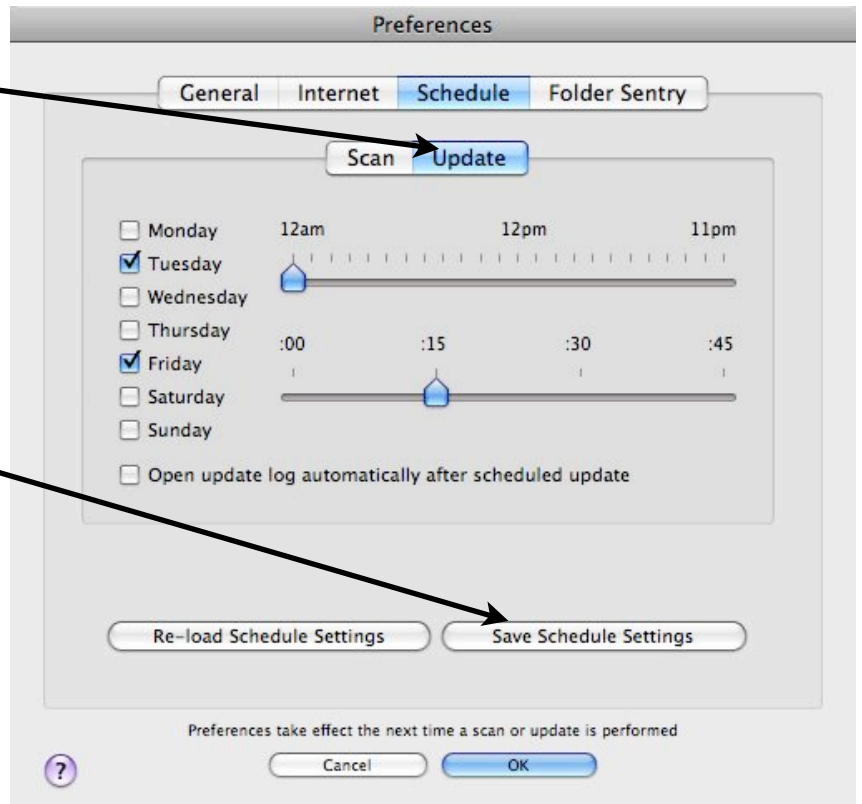
It is extremely important to schedule virus definition updates regularly. Screening of incoming files is seriously compromised if your virus information is out of date.

Go to the main window and click on Preferences.

Click on Schedule



Now click on Update



Set the days and times for automatic updates. They usually take less than a minute, so scheduling during inactive hours is not critical.

When you are through, click here. Again, DON'T click the OK button until after you have clicked Save Schedule Settings

If you just click the OK button, your schedule changes will NOT be saved.

Virus Scans

You can do manual or periodic scheduled scans of folders to find any viruses that may already be there.

General ClamXav Scanning Considerations

- Scanning is slow. Some types of file will be faster than others, but here is a rough guide obtained by scanning my Applications folders:

iMac, 2.4 GHz Intel core duo	3.6 minutes/Gigabyte
iBook, 1.2 GHz G4	16 minutes/Gigabyte

- The method of selection of folders to be scanned is limited and less than user-friendly.
- The good news is that with the current state of viruses that can infect the Mac (essentially none) it is not critical to scan extensively or often.
- File type limitations

ClamXav cannot scan virtual disks nor Smart Folders.

Disk image files, such as .dmg, .toast, .sparseimage and .sparsebundle will look like they are being scanned, but the actual contents will not be scanned unless the file is double-clicked and mounted on the desktop.

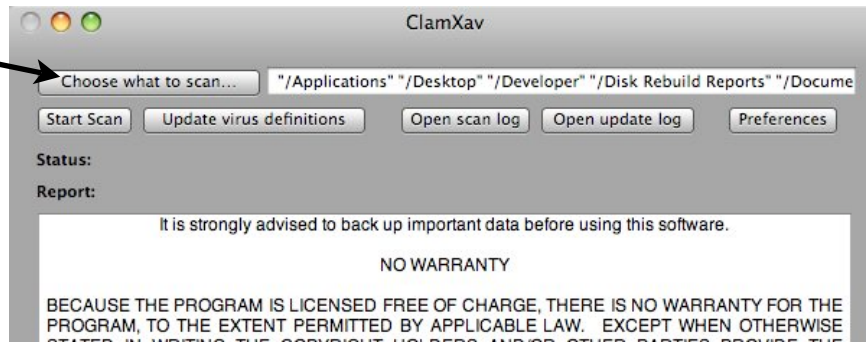
However, compressed archive files like .zip and .sit are scanned correctly without uncompressing them.

- With any Anti-Virus software, it is not a good idea to abort a scan in an abnormal manner; for instance by shutting off your computer or doing a force quit. These programs operate at a deep level in the disk and file structure of your data, and there is the potential for data loss or corruption. (*Back up your data!*) You should only abort a scan by using the mechanism built into the AV software. For Folder Sentry scans, this is done with "Abort Scans" in the pull-down menu under the Menu Bar icon. For ClamXav scans, this is done with the "Stop Scan" button in the main window or "Stop" in the File menu.

Manual Scan

Initially, it is a good idea to scan your entire computer. (*Back up your data!*) This will typically take between 5 and 20 hours, depending on the speed of your computer and the amount of data to scan. You probably want to do it overnight when your computer is not busy.

In the main ClamXav window, click on "Choose What to Scan"

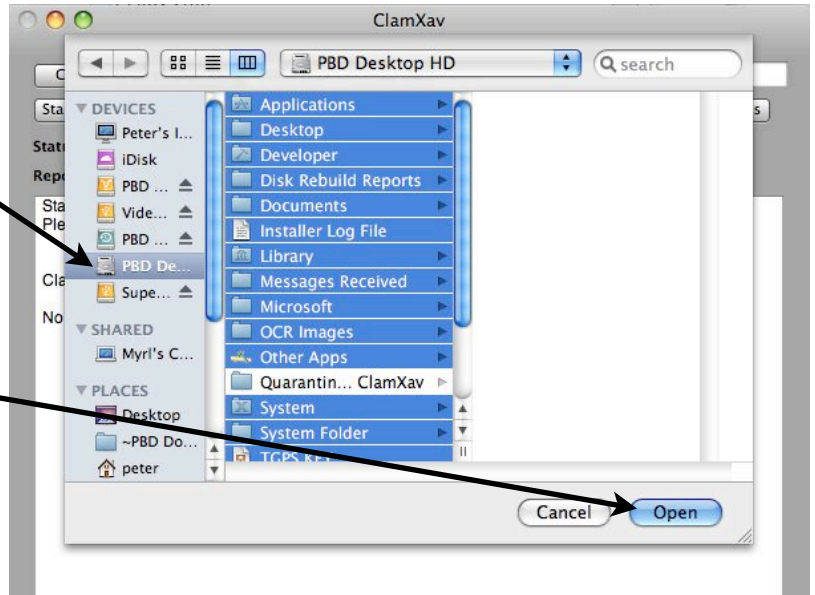


A file selection window will open.

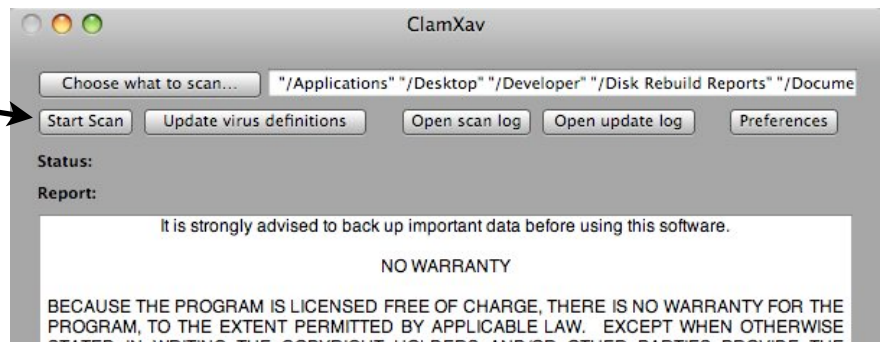
Navigate to your main hard drive

ClamXav will not allow you to choose the Hard Drive itself, but you can use Command - Click or Shift-Click to choose some or all of the folders in it.

After you have selected the folders, click Open

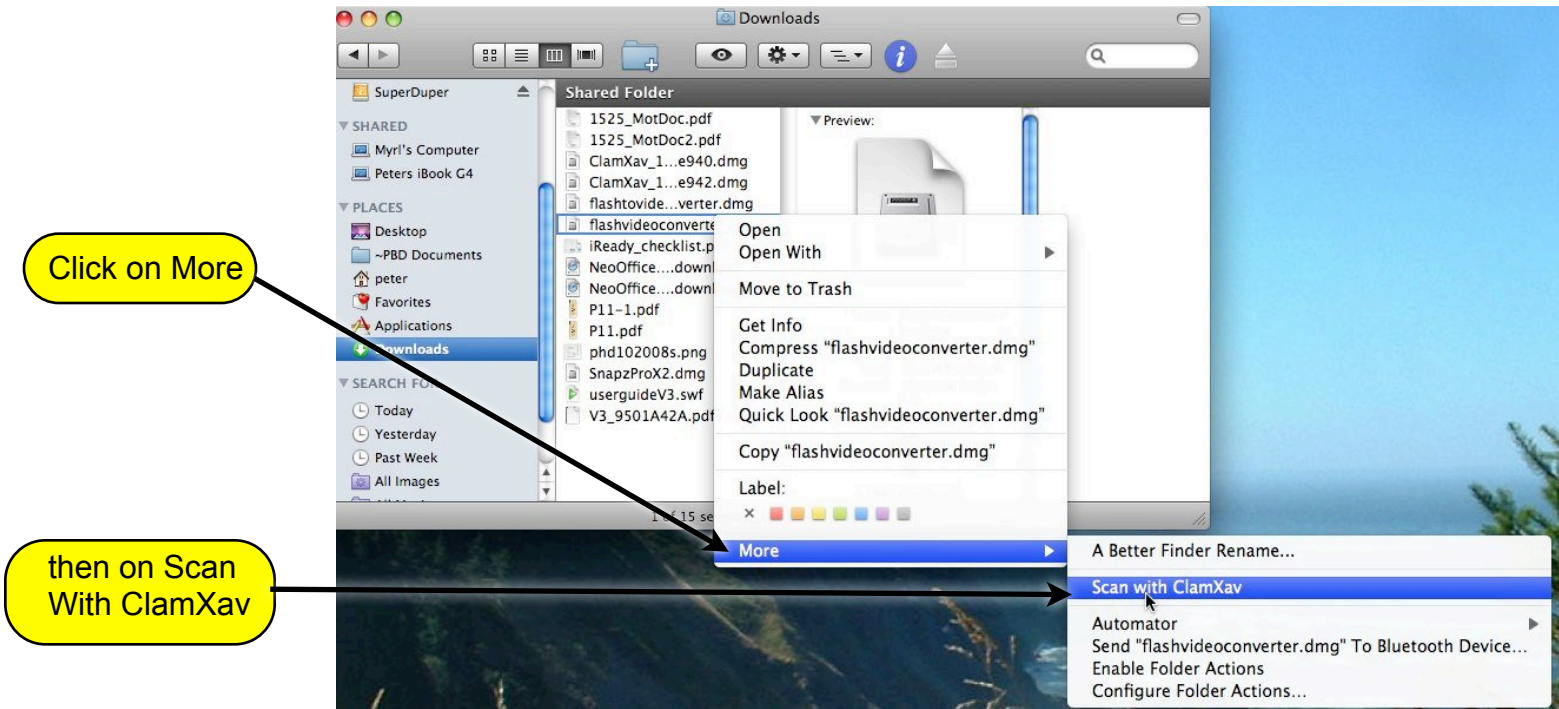


Click on Start Scan

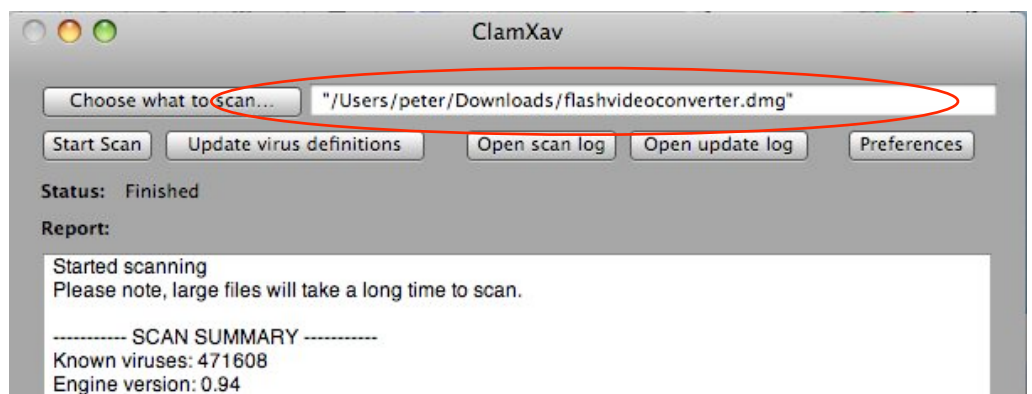


Manual Scan Via Contextual Menu

If you have installed the plug-in (p. 2) you can scan a single suspicious file, or a whole folder if you wish, from the contextual menu that appears when you right-click or control-click the file.



The main ClamXav window will open and the scan will start. Note however, that "Choose what to Scan" has been changed to the file being scanned. If you are running scheduled scans (discussed in the next section), you will have to change it back to the folder(s) you normally scan.



Manual Scan via Drag and Drop

If you keep ClamXav in your dock or put an alias of it on the desk top, you can also scan individual files or folders by dragging and dropping them on the ClamXav icon.

Scheduled Scans

What Folder(s) to scan?

This is the big question, and there isn't very much guidance out there on the internet that I can find.

Given the minimal threat to the Mac, a complete scan is overkill in my opinion. If you are really worried about viruses (as ex-PC users understandably tend to be) then you could do this periodically at night.

If you have Folder Sentry protecting the usual entry points (p. 4 & 5) then you should be safe there. However, you could schedule scans of these folders as "insurance". Unfortunately the limitations of the "What to Scan" choosing process makes it impossible to select multiple folders unless they are subfolders in the same folder, as in the full computer scan example, pp. 7 & 8. Instead, you could choose *Home/Library*, which contains the mail inboxes (plus many other folders and files), and *Home/Downloads*.

Since at present virtually all of the 100,000+ viruses out there are for Windows, if they do get into your Mac, they are just going to sit there and not infect any files. The only thing I really worry about is forwarding one contained in an email or email attachment, so for insurance the only scheduled scan I do is of *Home/Mail* and *Home/Mail Downloads*, even though Folder Sentry should catch any viruses when they arrive.

How to Schedule Scans

After choosing what to scan,

Click on Preferences

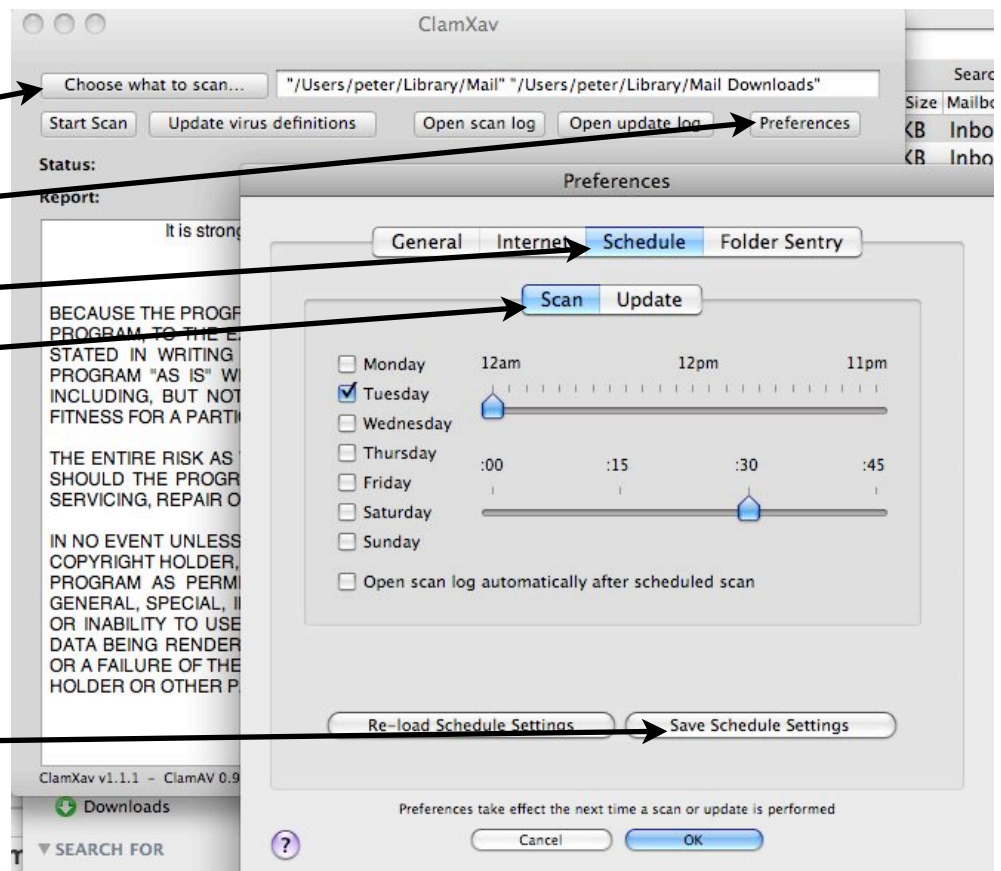
then click on Schedule

and then on Scan

Set the days and times for the scan. If you are scanning on the same days as scheduled Updates (p. 6), schedule the scan at least 15 minutes after the update so you are scanning with the latest virus definitions.

Again, click here *first*

and then on OK or your schedule settings won't be saved.



Special Situations

Some strategies to use if:

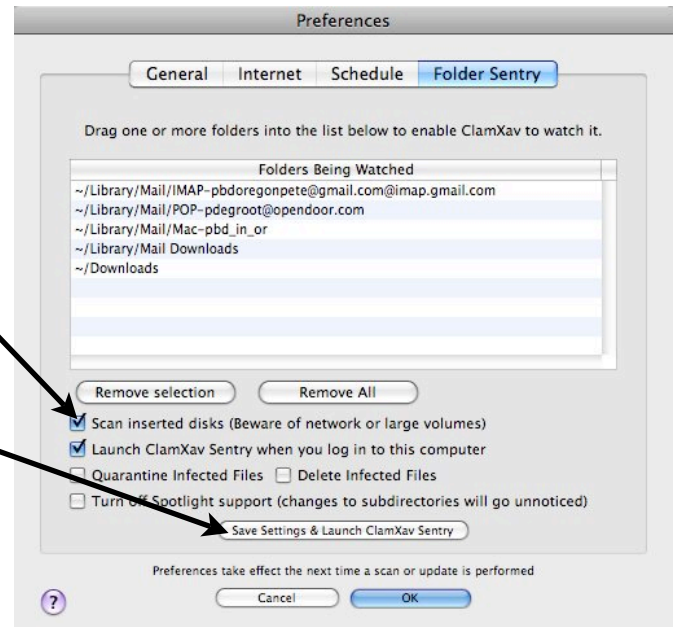
- **you often get files on Flash drives/cards, CDs, DVDs or portable Hard drives from other users**

a) Scan everything on any mounted disk with Folder Sentry:

!
!

Back in Preferences/Folder Sentry check the box marked Scan inserted disks

then click



This will scan all of the above media types when they are mounted (plus any disk images you mount on the desktop). It scans the whole thing, which can take a lot of time (about 4 minutes to scan a full data CD on my Intel iMac, for example), and it scans every mounted disk or flash card, which can get really annoying. However, you can abort the scan in the pull-down menu of the Folder Sentry icon in the top Menu bar.

b) Scan selected items with Folder Sentry:

Create a special folder on the desktop (called VirusCheck, for example) and add it to the folders watched by Folder Sentry (p. 4).

After mounting the disk, open it and drag the items you want checked into the special folder before moving them elsewhere on your machine.

c) Scan individual items with the Contextual Menu command or Drag & Drop

Right-click on the selected item (file or folder) and scan it with the Contextual Menu scan command or drag and drop the item onto the ClamXav icon (p. 9). You can scan it right on the mounted medium before you copy it to your computer. But remember that you will have to fix the "Choose what to Scan" Field (p. 9) if you are running periodic scheduled scans.

- you often receive files via iChat

- a) Create a special folder to put the items into before putting them elsewhere as in b) above.
- b) Scan the items with the Contextual Menu command as in c) above or with drag & drop (p. 9).

- you are running Windows on your Mac.

Your virtual Windows machine is just as vulnerable to all the viruses out there as any real PC, but they will only affect the virtual machine, not your Mac.

Note that if a Windows virus does get into the Mac side from an email, download, etc. it cannot "migrate" to the Windows virtual machine unless you deliberately move it there, and vice-versa.

ClamXav on your Mac doesn't provide any protection for your Windows virtual machine because it can **not** scan the virtual hard drive associated with the Windows machine.

Solutions:

- If you only use your Windows virtual machine occasionally, and never or seldom connect to the internet or receive email on it, Clamav (without the X) is a version for Windows that is also free.
- If you use your Windows virtual machine more like a real PC and download files and email, then you should spend the money for one of the commercial, heavy-duty antivirus applications for Windows.

Additional ClamXav Information

There are a few purported "Tutorials" out there but most are bad videos on YouTube and elsewhere showing only how to install ClamXav.

The best tutorial I have found is from the Rutgers University Computing Services department. <http://computing.camden.rutgers.edu/macintosh/clamxav.php> It is a little out of date. The warning about Firefox downloads doesn't apply to the current versions of ClamXav (1.1.1) and Firefox (3.0.3).

There is more information on www.clamxav.com, especially in the Documentation and FAQ sections and in the Support Forums.

Donation

If you find ClamXav useful, please consider making a donation on the website. While not as polished and comprehensive as the commercial ware, it is good basic antivirus software and a pretty awesome accomplishment for being created and maintained by a single person, Mark Allan.