

Virus Scanning

Checking files uploaded via Rumpus for viruses.

One of the primary uses of Rumpus, of course, is to allow varied and remote users to transfer files to your network. And since Rumpus can accept uploads from a variety of client platforms, the threat of transferring a virus is very real, even though Mac OS X generally suffers from fewer viral attacks than some other operating systems. In many cases, it is therefore important to scan uploaded files for viruses, and deal with them accordingly.

It is important to point out that Rumpus does not include a built-in anti-viral solution, but rather can be used in conjunction with dedicated solutions provided by other companies and organizations. By relying on dedicated third party software, you get the benefit of choosing among several high-quality, aggressively maintained virus detection packages, with only slightly more cumbersome (though also more flexible) configuration and setup.

Installing The Anti-Viral Software

You will first need to download and install whatever anti-viral software you decide to use. The only requirement for your choice is that there be a command line interface to trigger a virus scan, which most OS X-compatible virus detection packages offer. One good and inexpensive choice, which will be used as an example below, is ClamAV. A pre-compiled version of ClamAV is available in a package called ClamXav, at the URL below:

<http://www.clamav.net/>

<http://www.clamxav.com/>

These and other possible software options can also be found on any of the Macintosh software tracking sites such as MacUpdate (“www.macupdate.com”) and VersionTracker (“www.versiontracker.com”).

Whatever your choice, install the software as described in the documentation that accompanies the application. Next, open the Terminal and perform a scan of a single file. Be sure to include directives that tells the virus scanner what to do with infected files, where to log activity, and so on. Again, details on how to do this should be included in the anti-viral software’s documentation. If you are using ClamAV, for example, the following shell command will scan the file “somefile”:

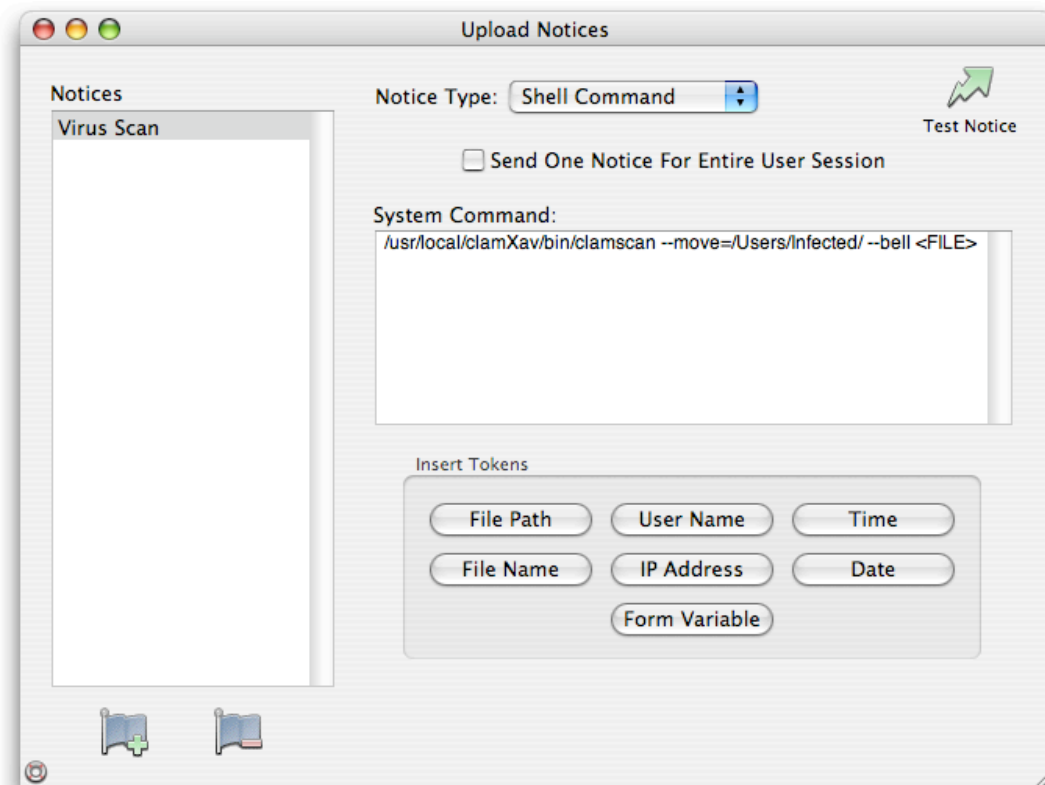
```
/usr/local/clamXav/bin/clamscan --move=/Infected/ --bell somefile
```

This command triggers ClamAV (“clamscan”), tells it to move infected files to the “Infected” folder, sounds an audible chime when an infected file is found, and specifies the file to be scanned. The file to be scanned should be specified as a full path, so when testing your virus scanning software, you will probably want to drag your test file into the Terminal window to complete the command, which will append the full path to the file as if you had entered it manually.

Configuring Rumpus

Rumpus will essentially execute a shell command, triggering the virus scan in exactly the same way you do using the Terminal, each time a file is uploaded. So, the first step in configuring Rumpus is to finalize an example of the shell command you would like executed.

Once your virus scanning shell command is set to scan a sample file, open the Upload Notices window in Rumpus and create a new notice. Set the “Notice Type” to “Shell Command”, and then copy and paste the command example from the Terminal into the “System Command” text area. Next, replace the sample file path with the “<FILE>” token, by selecting the file path and clicking the “File Path” button. When you are done, the Upload Notice will look something like this:



With the Upload Notice completed, close the window and open the “FTP Settings” window. Flip to the “Admin” tab and select the virus scanning Upload Notice you just created from the “Global Upload Trigger” pop-up menu. This will cause Rumpus to trigger the shell script that performs the scan for each and every file uploaded through Rumpus.

Final Notes

Please read the documentation that accompanies your virus scanning software carefully. Scans of files uploaded through Rumpus will only be as complete and accurate as the software, and the shell command that triggers it. Also, be sure to check for software and virus profile updates on a regular basis, to ensure that your server will continue to detect newer viruses that may be released.

As always, if you have trouble please send e-mail to “support@maxum.com”. Please note that Maxum is unable to provide detailed support for third party virus scanning software products, but we will be happy to help you integrate them for use with Rumpus.