

ClamAV For Windows

Free Anti-Virus Software For Windows Servers

Author: Brian Bruns <bruns@2mbit.com>

Date: 3/07/2005

Version: 1.0a

About ClamAV For Windows

ClamAV For Windows is a port of the popular and powerful ClamAV for UNIX/Linux machines to Win32 systems. It is known to support Windows NT 4 SP6, Windows 2000 SP4, Windows XP SP2, and Windows 2003. It may also properly work on Win9x (including Windows ME) systems as well, but is completely unsupported.

About The SOSDG

The SOSDG <<http://www.sosdg.org>> is a group of individuals that work towards common goals for the benefit of the Internet community. These goals include the inexpensive/free hosting of Open Source/Free Software projects, other not-for-profit/non-profit groups, porting of useful applications to other platforms to encourage further use, and more.

What Is ClamAV Best Used For?

ClamAV For Windows is best used on servers when integrated with programs that properly recognize it. There is a list of programs that support ClamAV for Windows on the main SOSDG website page for the program <<http://www.sosdg.org/clamav-win32>>.

What Separates ClamAV From Other Antivirus Programs?

ClamAV is open source and 100% completely free, including definition updates. There is no fee now or ever for using ClamAV, and is released under the GPL. For more information on the license regarding ClamAV For Windows, see <<http://www.sosdg.org/clamav-win32/copying.txt>>.

How Can I Use ClamAV?

Scanning for viruses is fairly simple and straight forward. Start a 'cmd' prompt and type:

```
C:\clamav-devel\bin\clamscan.exe <path to file to scan>
```

Please note that because of oddities between Windows and UNIX/Linux standards, you must do one of the following with your paths you specify to ClamAV:

1. Replace \ with / in your paths - ie: C:/clamav-devel/test/clam.exe

2. Double your backslashes - ie: C:\\clamav-devel\\test\\clam.exe
3. Use Cygwin Cygdrive notation - ie: /cygdrive/c/clamav-devel/test/clam.exe

When run correctly, you will see an output like the following:

```
C:\\clamav-devel\\test\\clam.exe: ClamAV-Test-File FOUND
```

```
----- SCAN SUMMARY -----  
Known viruses: 31322  
Engine version: devel-20050302  
Scanned directories: 0  
Scanned files: 1  
Infected files: 1  
Data scanned: 0.00 MB  
Time: 3.250 sec (0 m 3 s)
```

As you can see from the above output, ClamAV has detected one of the test files as a virus successfully.

Updating Your Virus Definitions

To update your virus definitions, all you need to do is run the 'freshclam' program. You can do this by going to the ClamAV menu item in the Start Menu under Programs, by double clicking on the exe file in C:\\clamav-devel\\bin, or on the command line:

```
C:\\clamav-devel\\bin\\freshclam.exe
```

Please remember that you need to have an active internet connection in order to update the definitions! You can also run this every few hours using the Task Manager which ensures that you always have the latest virus definitions. Please do not check more than once every 2-3 hours though, as this will put unnecessary load on the ClamAV file servers!

Editing Misc Settings For FreshClam and the clamd Daemon

All configuration files are located in the C:\\clamav-devel\\etc directory and can be edited with notepad, or any other text editor that can write plain text files. Please do not use WordPad, Microsoft Word, or other Word Processing applications to edit these files, as it will add extra junk to the file that will cause ClamAV to stop functioning.

If you would like to learn more about the settings, you can read the PDF document which is included with the ClamAV documentation:

```
C:\\clamav-devel\\docs\\clamdoc.pdf
```

That document also contains full details on how to use the more advanced features of ClamAV.

Starting And Stopping The clamd Daemon

The clamd daemon is used for higher speed scanning, and is commonly used when ClamAV is scanning for viruses on a mail server.

The recommended way to start clamd is by running the start-clamd.bat batch file in the C:\clamav-devel directory. You can do this quickly by using the 'Start Clamd' item under ClamAV in the Start Menu. You can also stop clamd in the same way (by selecting Stop Clamd or using the stop-clamd.bat batch file).

With the clamd daemon running, you can now use clamdscan.exe instead of clamscan.exe, which will scan using the clamd daemon. This is a much more efficient way of scanning when you have a large amount of files or e-mail to scan.

Return Codes For ClamAV

Most programs that use ClamAV, rely on the return code to determine if the file scanned is a virus or not. Depending on which version of the Cygwin1.dll you use, these codes may be different.

```
=====
      Status          | <= Cygwin v1.5.12 | Cygwin v1.5.13
=====
Virus not found     |          0         |          0
Virus found         |          1         |         256
Error with scan     |          2         |         512
File not found      |          56        |        14336
=====
```

Please note that this change was not intentional on the ClamAV side, but rather because of a move by the Cygwin developers. All return codes are multiplied by 256 in Cygwin 1.5.13 before being passed back to Windows. This is unfortunately a change that the SOSDG has no control over and one that the Cygwin developers appear to be unwilling to roll back.

To determine which version you have, either look at the version property of the cygwin1.dll via Explorer, or when running the installer, check the version number in the titlebar. Version 1.5.12 is identified by Cygw1512, and version 1.5.13 is identified by Cygw1513.

Using ClamAV In Other Directories Besides C:\clamav-devel

ClamAV will not run properly in other directories besides C:\clamav-devel unless you specify full paths on the command line to the directory where you moved ClamAV.

```
clamscan.exe --database=e:\ClamAV\share\clamav  
--tempdir=e:\clamav\tmp --log=e:\ClamAV\log\clamav.log
```

This is a limitation of Windows, mostly due to the fact that Windows does not follow directory standards that UNIX/Linux follow (there are no 'a' or 'c' drives on UNIX/Linux, just drives mounted directly to paths such as /usr/local/bin).

Please note that moving ClamAV is completely unsupported and not recommended. Also, ClamAV may not work right if the directory path has spaces in it.

A Final Note

Obviously, this is not full documentation on how ClamAV For Windows works, but it will help give you a starting point. Please check <<http://www.sosdg.org/clamav-win32/>> for more updates in the future!