

# Installation of ClamAV-SOSDG for XWall

By maga, 15. Aug. 2008, for the XWall forum (<http://www.xwall.us/phpBB3/index.php>)

After using several "bigshot" antivirus products with XWall, I settled with ClamAV. The main reasons are: Reliable and stable operation, really fast commandline scanning, decodes all common mail formats and archive types, virus name reporting, quick response times for new threats, service (daemon) mode operation, completely free (however, donations to the developers are welcome), excellent support from the user community.

## 1. Download current/latest software package here:

<http://www.sosdg.org/clamav-win32>

## 2. Install on your XWall machine:

Execute the downloaded installer, e.g. "clamav-sosdg-0.93.3-1a.exe"

Select the **Type of install: "Full"**

Leave the default Destination Folder

Wait for the update to complete

Close the installer

## 3. Exclude the ClamAV directory from your local On-Access Antivirus Scanner, including all subdirectories and files:

```
C:\clamav-devel\*.*
```

## 4. Edit C:\clamav-devel\etc\clamd.conf

Comment out the following lines by prepending a "#":

```
#LocalSocket /cygdrive/c/clamav-devel/clamd.sock  
#FixStaleSocket yes
```

Uncomment the following lines by removing the prepended "#":

```
TCPsocket 3310  
TCPAddr 127.0.0.1
```

Adjust the value of StreamMaxLength to the maximum allowed size of your incoming mails:

```
StreamMaxLength 25M
```

## 5. Edit C:\clamav-devel\thirdparty\runclamd\runclamd.ini

Uncomment the following line by removing the prepended ";":

```
AutoStart=Yes
```

## 6. Install the RunClamd service by executing:

```
C:\clamav-devel\thirdparty\runclamd\runclamd.exe -install
```

## 7. Start RunClamd Service by executing:

```
C:\clamav-devel\thirdparty\runclamd\runclamd.exe -start
```

## 8. Verify that the scanner service is running properly by checking the test files:

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

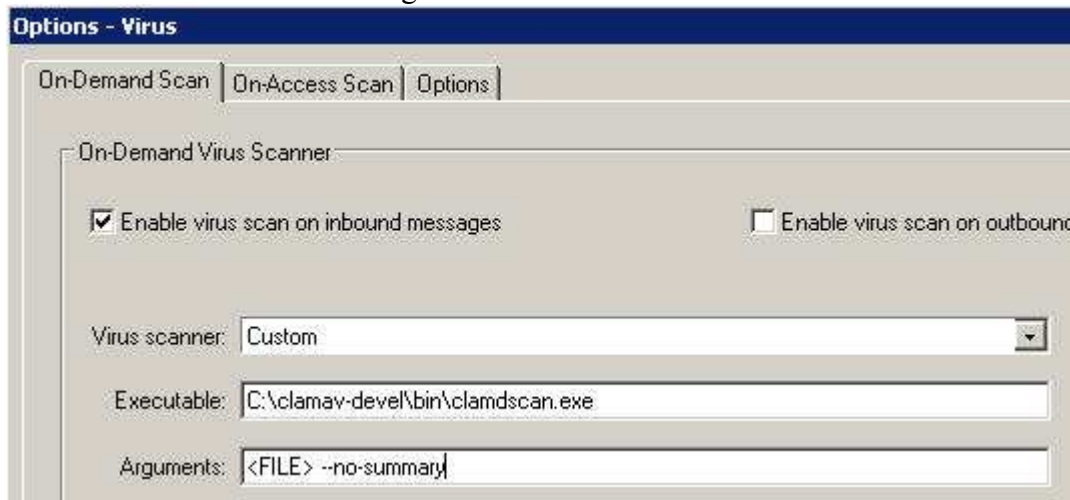
This should show several lines ending in ...FOUND.

## 9. Configure XWall to use the clamscan commandline scanner

Start MAdmin, Navigate to Options, Virus, On-Demand Scan

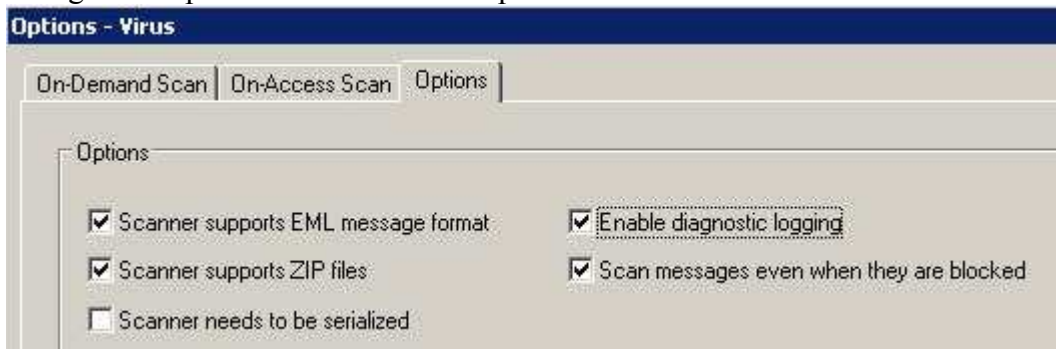
Enable virus scan on inbound messages

Enter the executable and the arguments as shown

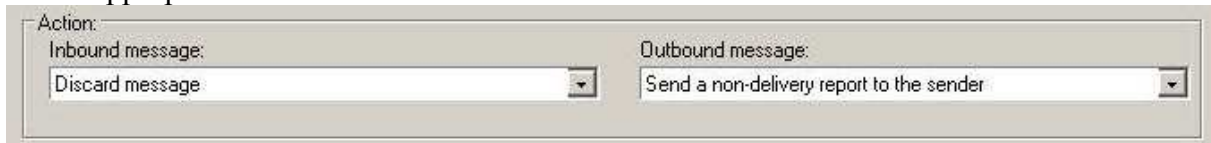


Navigate to On-Access Scan and **disable On-Access scanning**.

Navigate to Options and check these options:



Select appropriate actions for infected mails.



Enable virus statistics in MAdmin, Options, General, Statistics:



Close XWall Admin to save the configuration.

Add this line manually to your XWALL.INI:

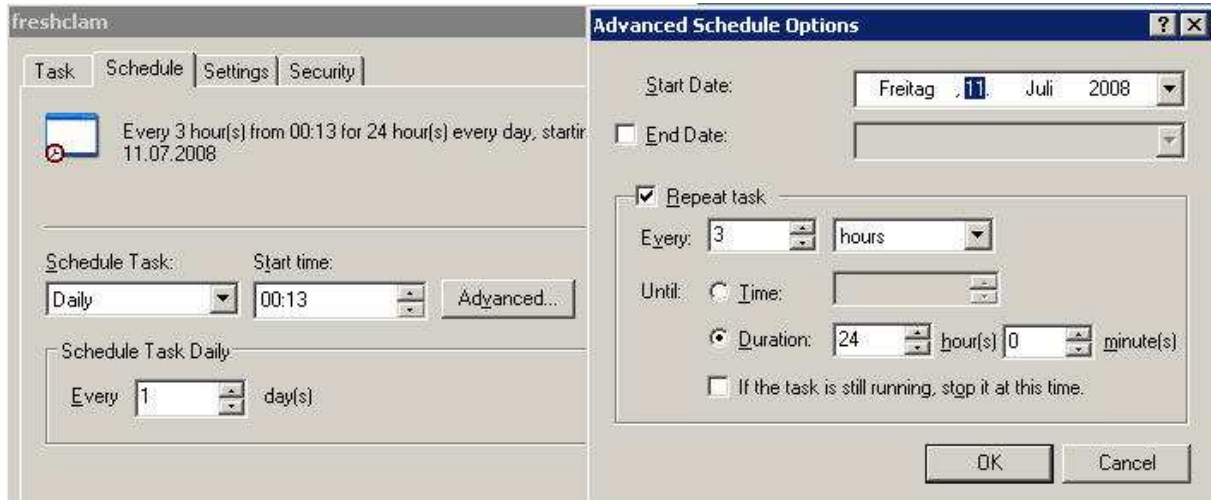
```
VirusScannerExitCode=Xxxxxxxx
```

XWall will restart automatically as soon as it notices the configuration changes.

## 10. Enable automatic updates of the antivirus definition files:

Add a new Task Scheduler Job on your XWall machine to run  
C:\clamav-devel\bin\freshclam.exe  
in regular intervals, e.g. every three hours.

Please choose a Start time with random minutes.

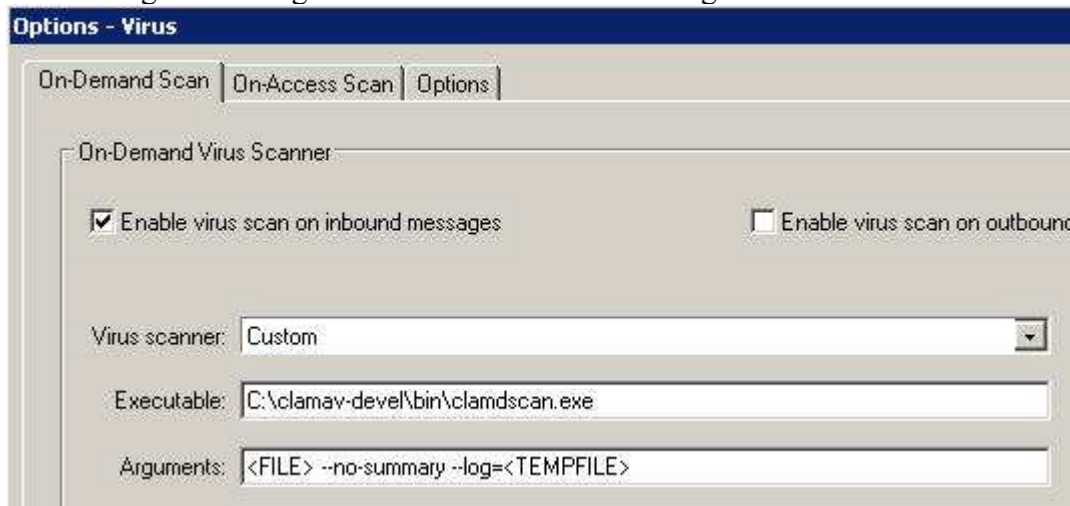


**11. To use virus reporting**, you have to add a few parameters to your configuration:  
(Skip this step if you do not need the virus names in your reports)

Download the zipped ParseReport script from here:  
<http://download.dataenter.co.at/ftp/demk/parsereport.zip>

Extract the VBS file to your C:\XWall directory.

Add the argument --log=<TEMPFILE> to the other arguments.



Add these two lines manually to your XWALL.INI:

```
VirusPostScanner=C:\WINDOWS\system32\cscript.exe  
VirusPostScannerPara=C:\XWALL\ParseReport.vbs <TEMPFILE> <MSGFILE> CLAMAV
```

XWall will restart automatically as soon as it notices the configuration changes.

## 12. Verify proper XWall-Antivirus operation

Send an mail containing an EICAR test virus to your XWall server and check the log:

**Either** copy the EICAR signature from [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm) paste it into a mail and send it to your server

**or** send an embedded EICAR test mail by using this web page: <http://tools.decluce.com/>



The screenshot shows a web interface titled "Virus Tools" with a sub-section "Test Messages". Below the title is a grey banner with the text "See how your mailserver reacts to Virus Emailing techniques". The form contains two input fields: "Enter your E-mail address:" with the value "user@example.com" and "Eicar file to send:" with a dropdown menu showing "eicarplain - Plain base64 MIME encoded". A "Submit" button is located below the second field.

(If you use Greylisting, you may have to try twice.)

This should result in your XWall finding the EICAR test virus.

In the logfile MB.LOG

```
08-08-15 19:57:03 00305: Virus: Scanning attachments...
08-08-15 19:57:03 00305: Executing C:\clamav-devel\bin\clamdscan.exe
c:\xwall\temp\%$TE9dalf --no-summary --log=c:\xwall\temp\%$TE9dall
08-08-15 19:57:03 00305: clamdscan.exe returned error level 1
08-08-15 19:57:03 00305: Executing C:\WINDOWS\system32\cscript.exe
C:\XWALL\ParseReport.vbs c:\xwall\temp\%$TE9dall c:\xwall\temp\%$TE9dalm
CLAMAV
08-08-15 19:57:04 00305: cscript.exe returned no error
08-08-15 19:57:04 00305: Virus: Scanner reported virus infection for
eicar.com (Found Eicar-Test-Signature)
08-08-15 19:57:04 00305: Spam: virus
08-08-15 19:57:04 00305: What: Discard message
08-08-15 19:57:04 00305: Why: Virus scanner reported an infection in
eicar.com
```

In the statistic file SVxyyzz.csv

```
"Date","Time","Type","From","Recipient","File","Virusinfo"
"08-08-15","19:57:04","I","webmaster-
vir@decluce.com","user@example.com","eicar.com","Found Eicar-Test-
Signature"
```

References::

[http://www.dataenter.co.at/doc/xwall\\_technical\\_resources.htm](http://www.dataenter.co.at/doc/xwall_technical_resources.htm)

[http://www.dataenter.co.at/doc/general\\_scanner\\_parse\\_report.htm](http://www.dataenter.co.at/doc/general_scanner_parse_report.htm)

<http://www.xwall.net>

<http://www.xwall.us>