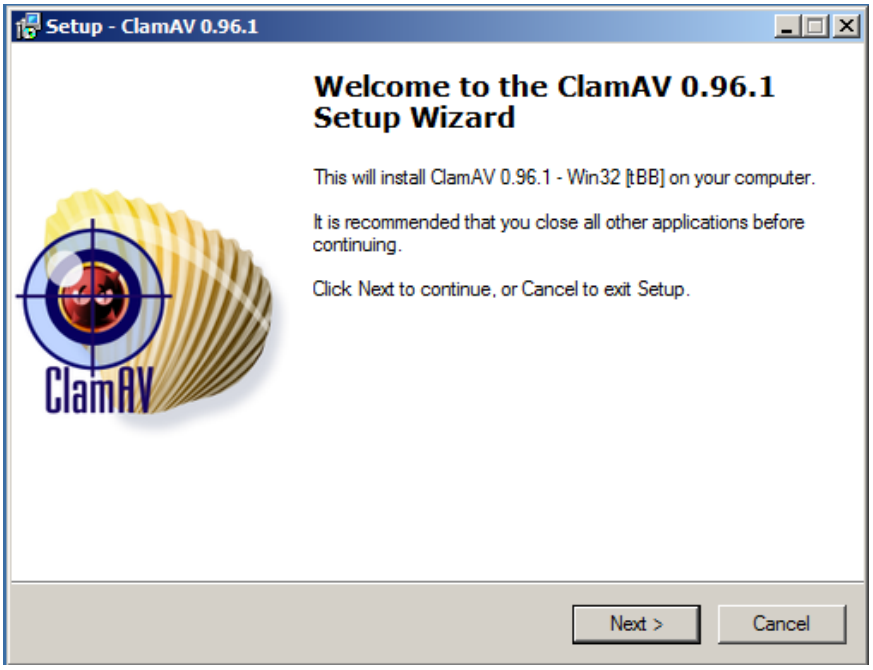
Installing ClamAV AntiVirus:

Download ClamAV from the website: http: // hideout.ath.cx/clamav/

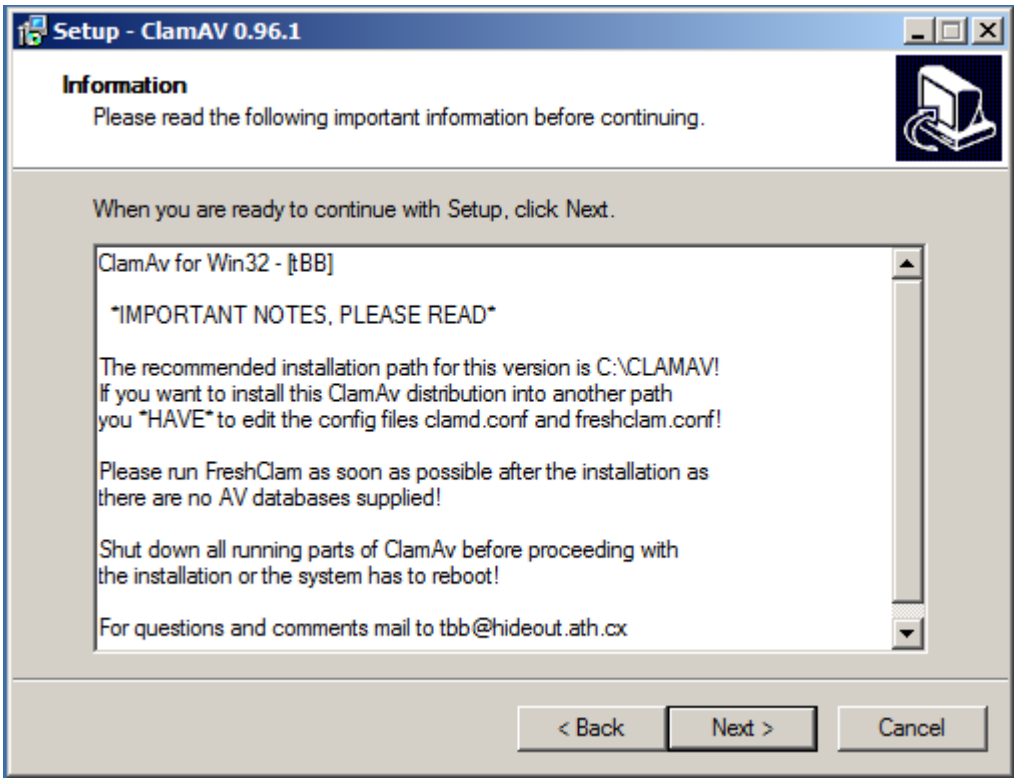
Start the installations Wizard.

Figure 1.



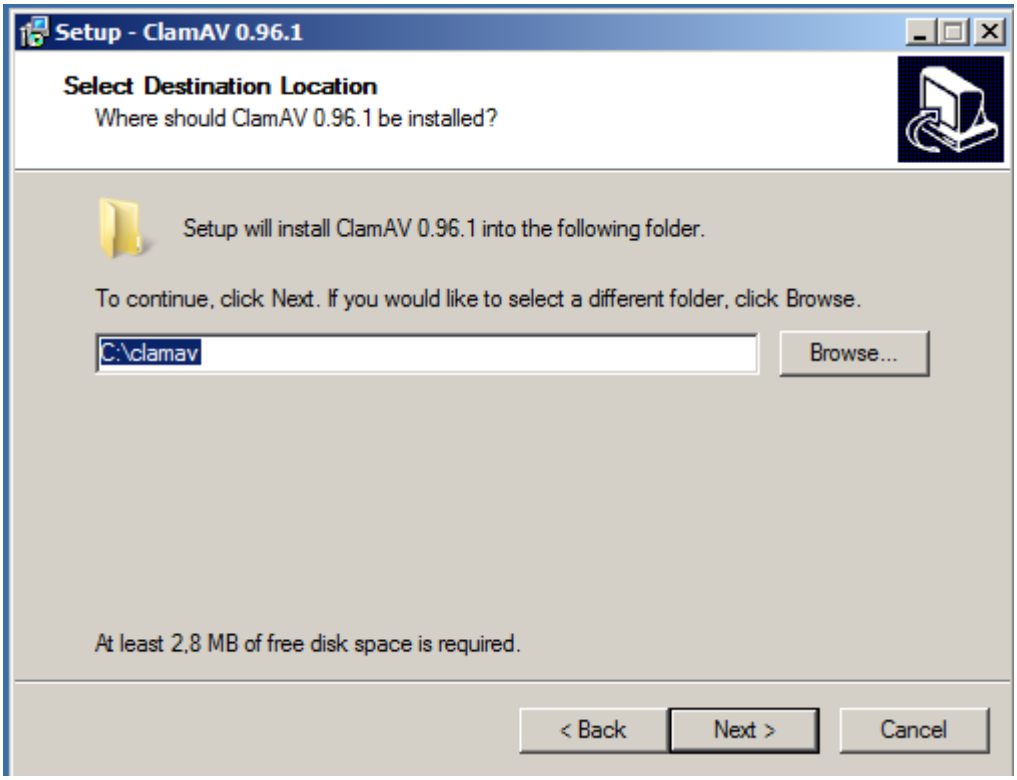
Click „Next“

Figure 2.



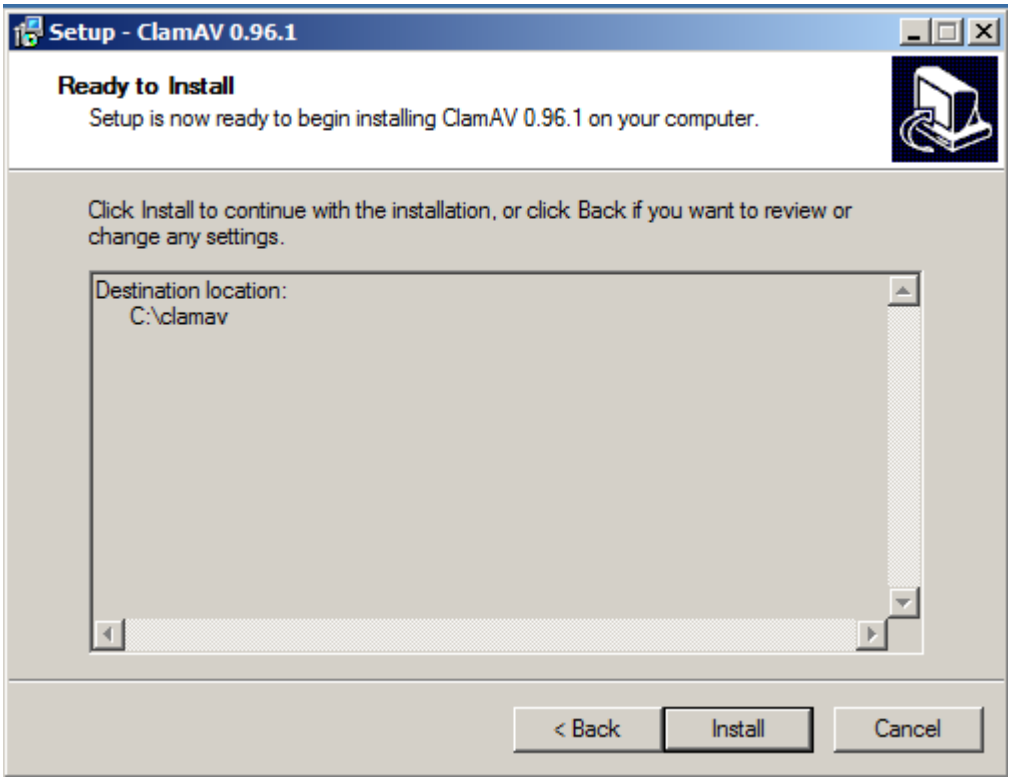
Click „Next“

Figure 3.



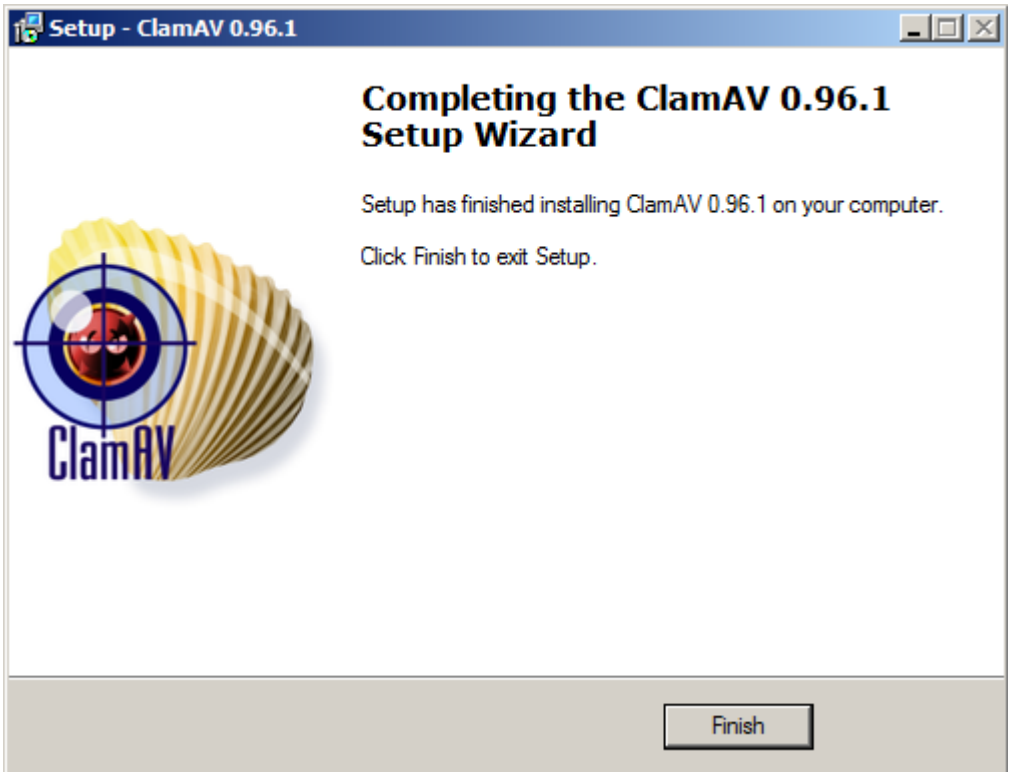
Use the default path: C:\clamav

Figure 4.



Click „Install“

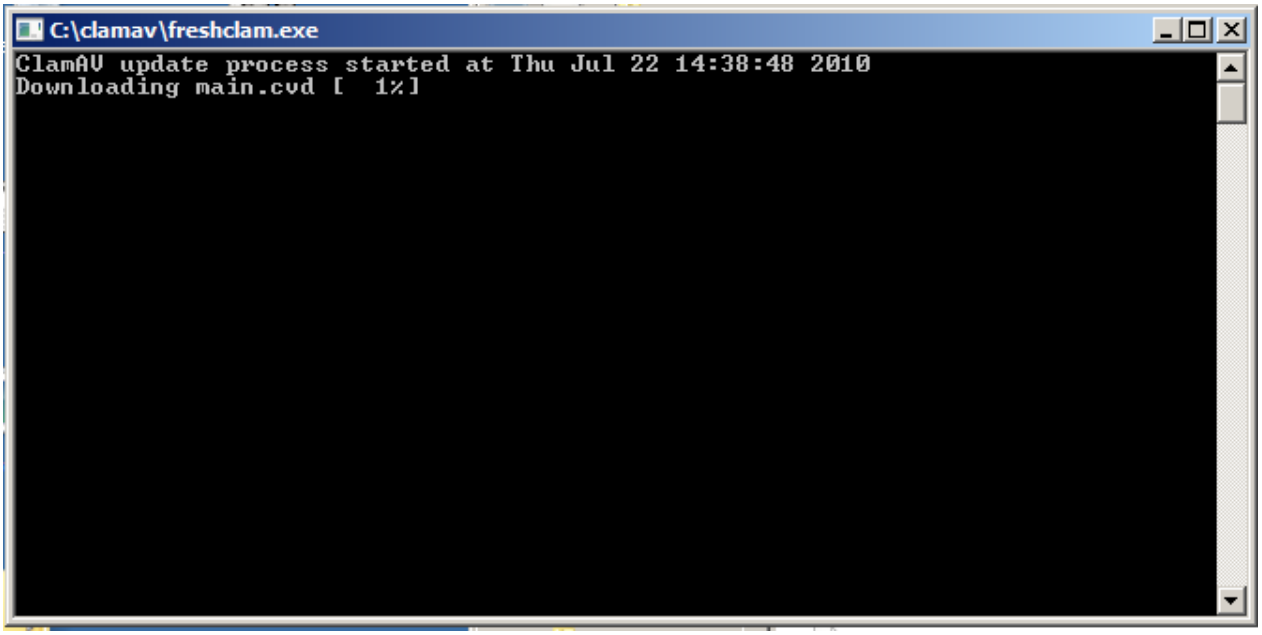
Figure 5.



Click „Finish“

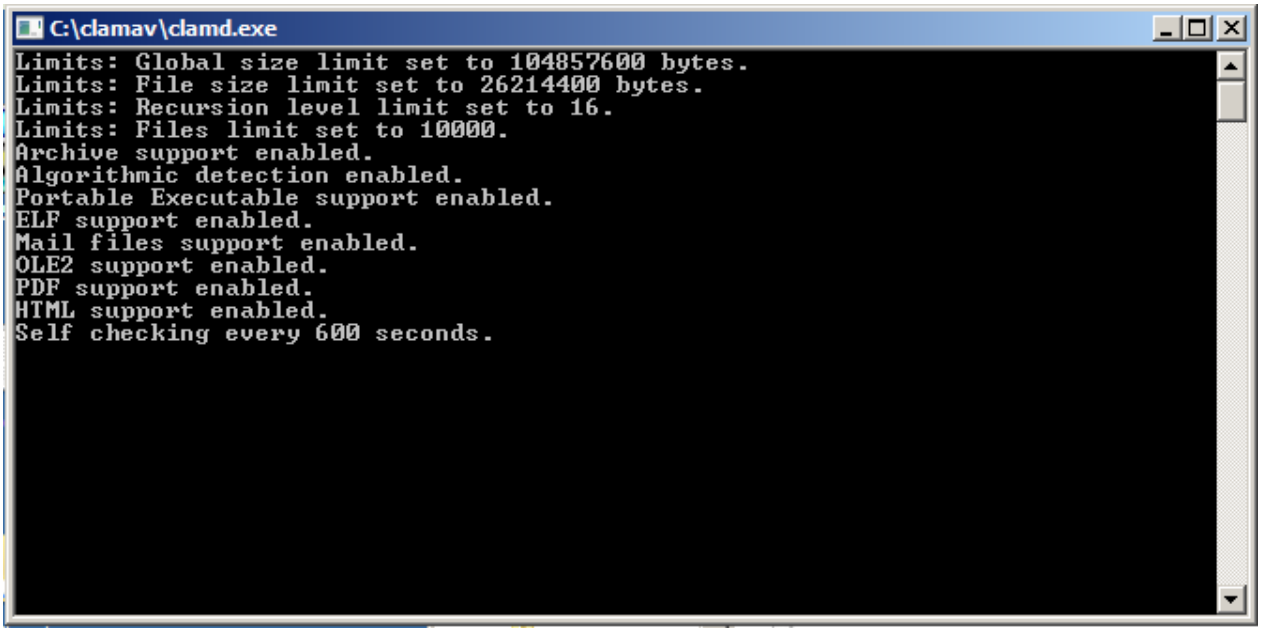
The installation of ClamAV AntiVirus is now complete. The first thing that needs to be done is open freshclam.exe (C:\clamav\freshclam.exe) to load the virus signatures.

Figure 6.



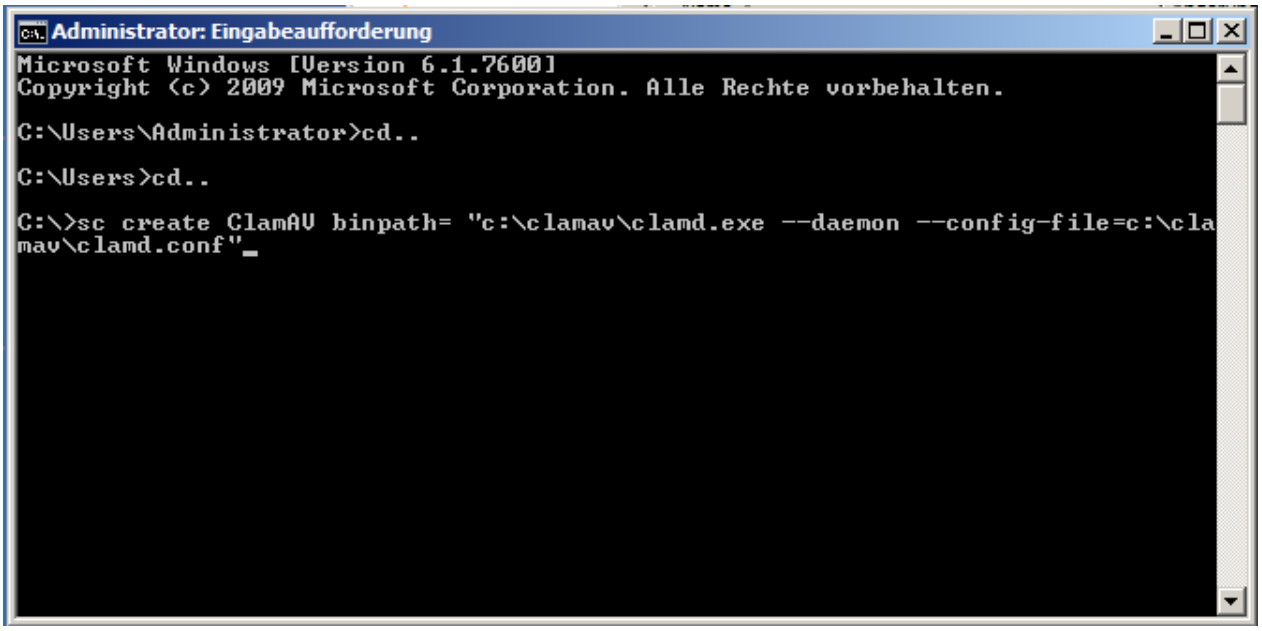
Before installing clamd.exe as a service it should be checked to see if it works. This is done to make sure nothing was corrupted during the download. Start clamd.exe (C:\clamav\clamd.exe)

Figure 7.



If the following dialogue loads in a cmd window then clamd.exe is working.

Figure 8.



Now both clamd.exe and freshclam.exe need to be installed as services. It doesn't matter in which order.

Open a cmd window.

step 1: >cd.. <enter>

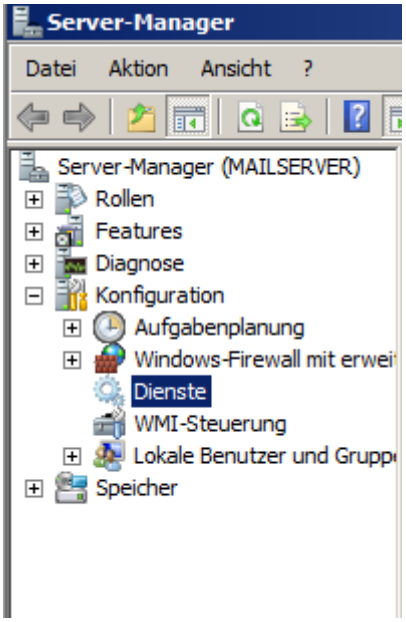
step 2: >cd.. <enter>

step 3: >sc create ClamAV binpath= "c:\clamav\clamd.exe --daemon --config-file=c:\clamav\clamd.conf"

<enter>

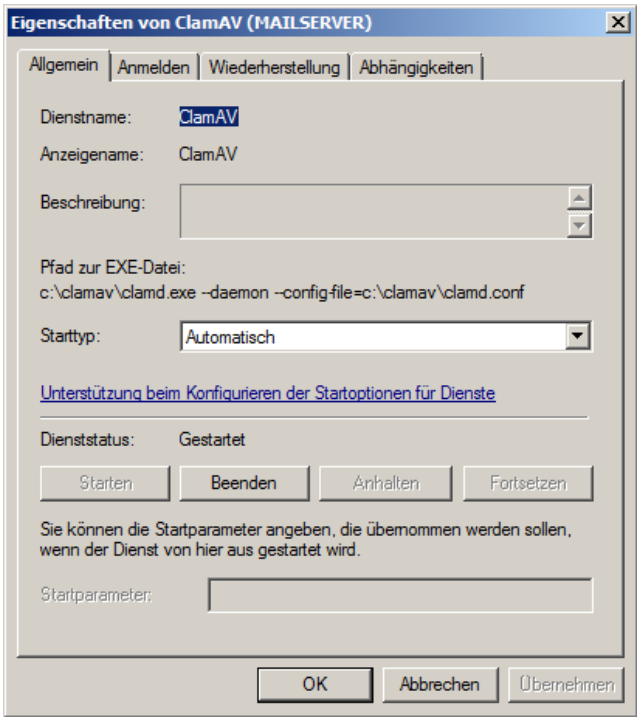
Give in the following commands to install clamd.exe as a service. Highlighted in RED is just the name the service will appear as, can be named anything. Open the Server-Manager and under configuration open services and ClamAV.

Figur 9.

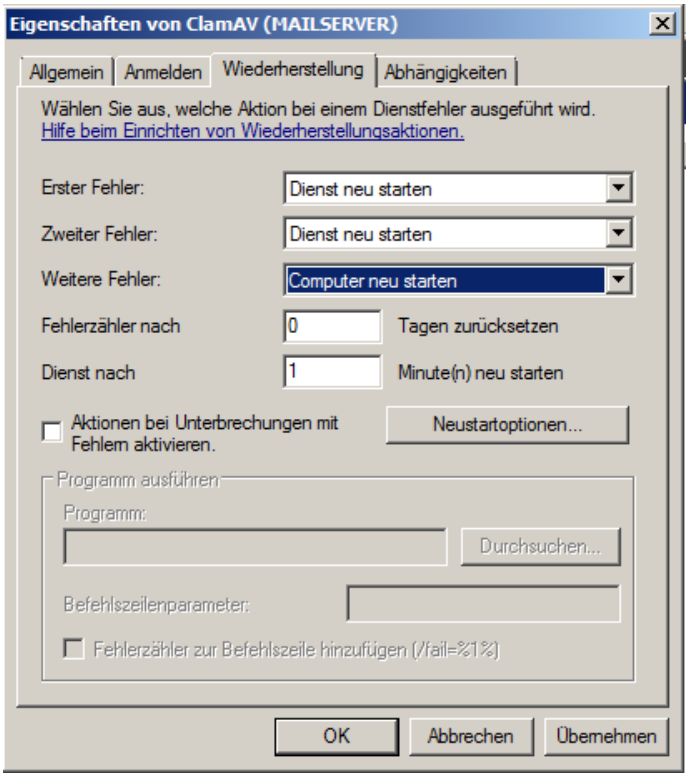


Before the service can be started some of the setting need to be changed. First the start type needs to be changed from manual to automatic so that the service starts when the computer boots.

Figur 10.



Figur 11.



Under the restart tab:

Erster Fehler (first failure): Dienst neu starten (restart service)

Zweiter Fehler (second failure): Dienst neu starten (restart service)

Weitere Fehler (further failures): Computer neu starten (restart computer)

Now clamd.exe is configured to run as a service.

With the same commands and configuration install freshclam.exe

Step 1: >cd.. <enter>

Step 2: >cd.. <enter>

Step 3: >sc create FreshClam binpath= "c:\clamav\freshclam.exe --daemon --config-file=c:\clamav\freshclam.conf"

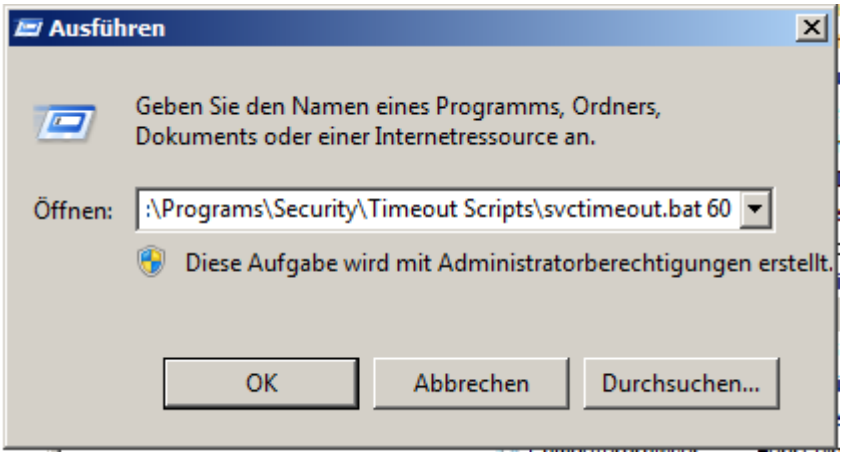
<enter>

Now both clamd.exe and freshclam.exe are installed as services but the timeout duration is too short so while booting the services will be unable to load. Therefore the timeout duration needs to be increased.

From the same website: von http: // hideout.ath.cx/clamav, download the svctimeout.zip and unzip the batch file.

Open a run window:

Figur 12.



Enter the path for the batch file and at the end give in the time in seconds.

Example: E:\Programs\Security\Timeout Scripts\svctimeout.bat 60

Now the timeout duration has been increased to 60 seconds this is usually sufficient.

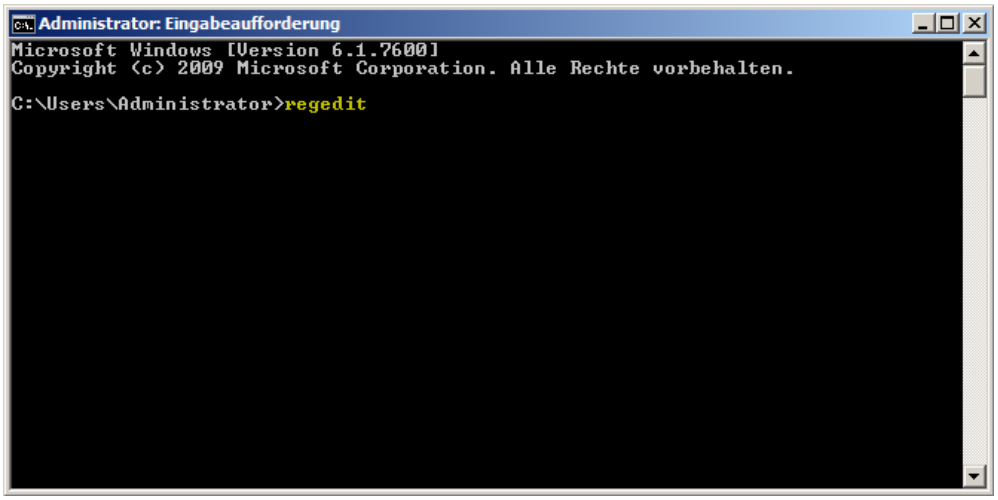
Now the logging functions for both clamd.exe and freshclam.exe need to be enabled. This is a good idea so that in the future when something goes wrong with the MailServer you can look into the log files to see if the problem is associated with ClamAV.

Open the .conf files (C:\clamav) for clamd.exe and freshclam.exe and enable the logging and log time functions by uncommenting them.

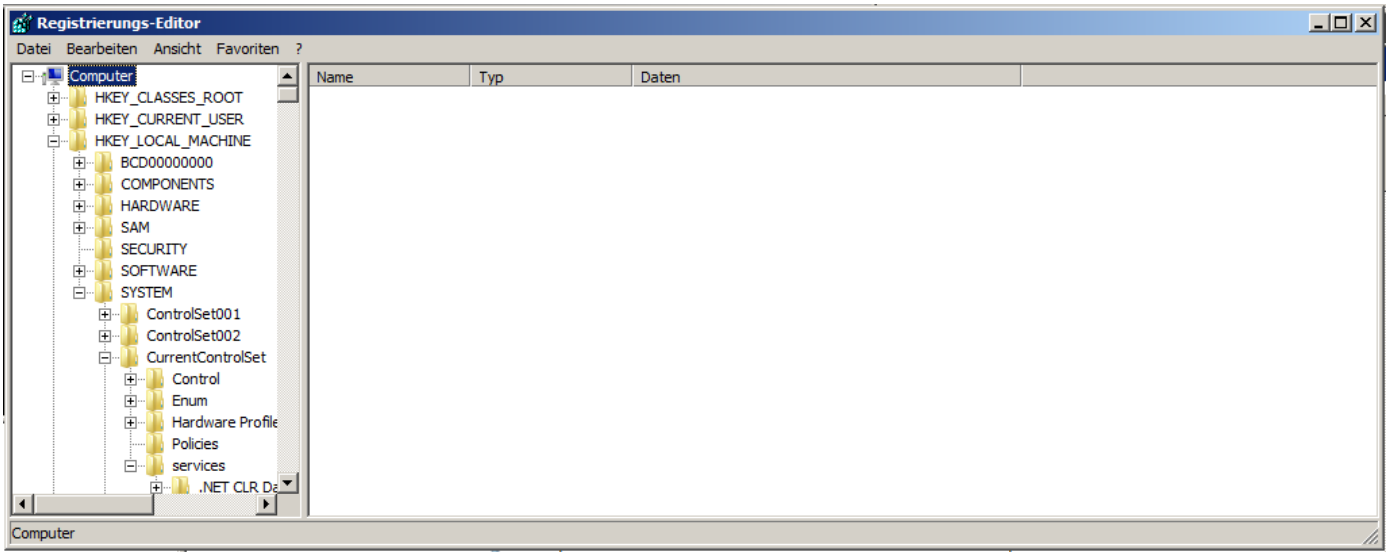
Now open the Server-Manager and start the services. If they start without failing then you are good to go.

The next step is to make some changes to the registry. This is always dangerous if you make a mistake so make a backup before you start this step. Open the registry by typing the cmd: regedit into a cmd window.

Figur 20.

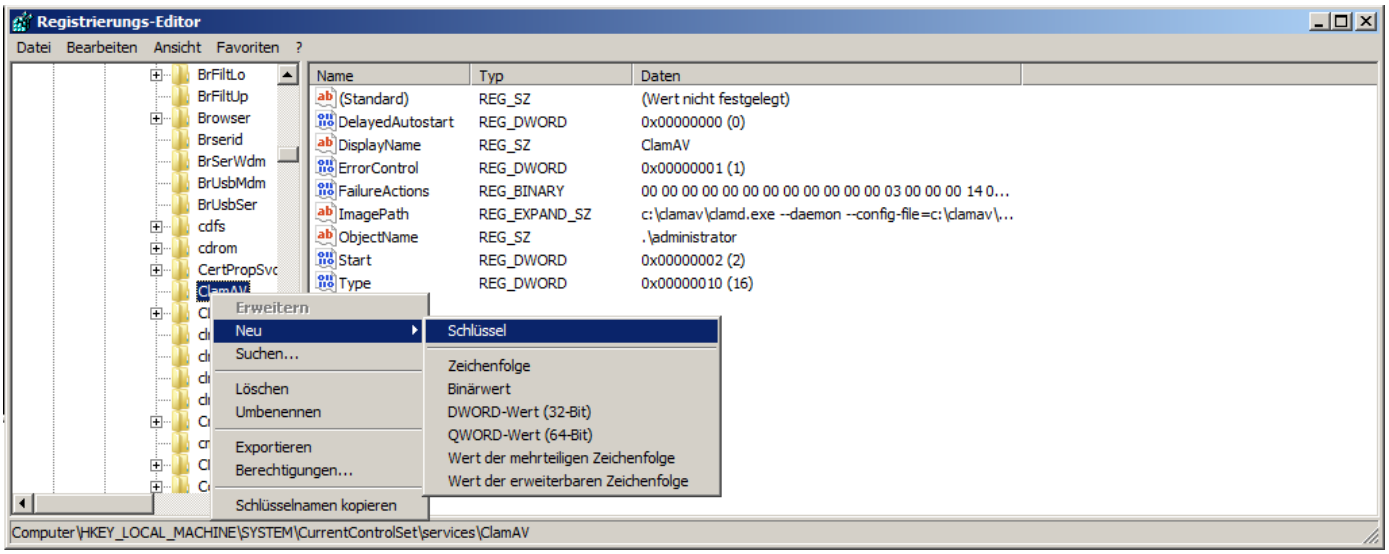


Figur 21.



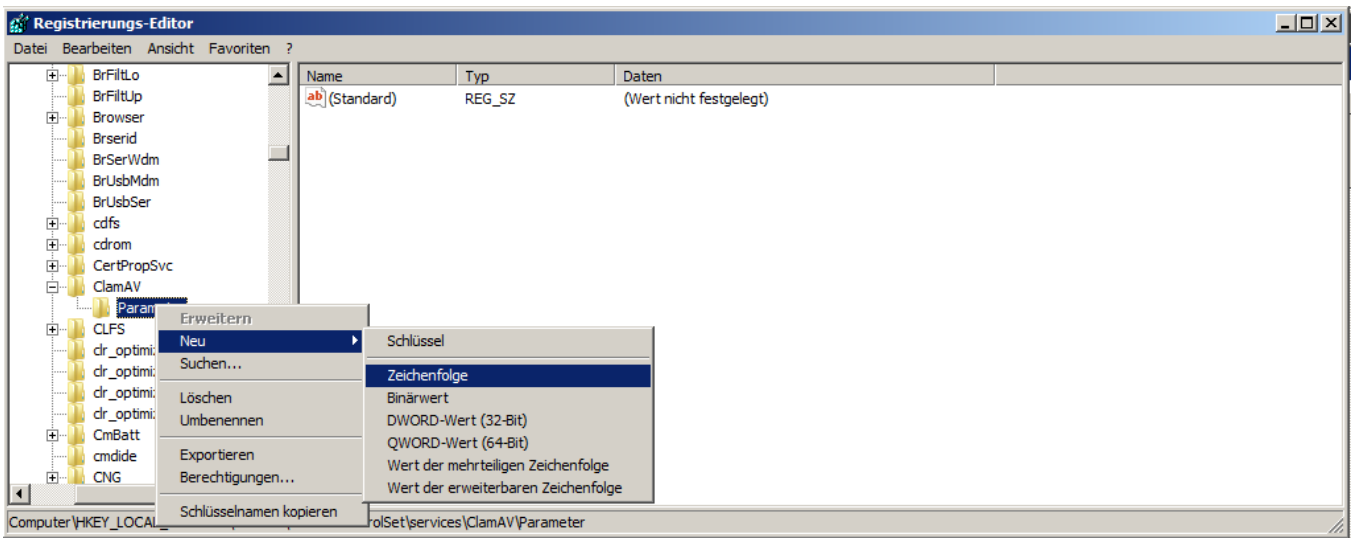
In the registry editor under open HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>services, ClamAV

Figur 22.



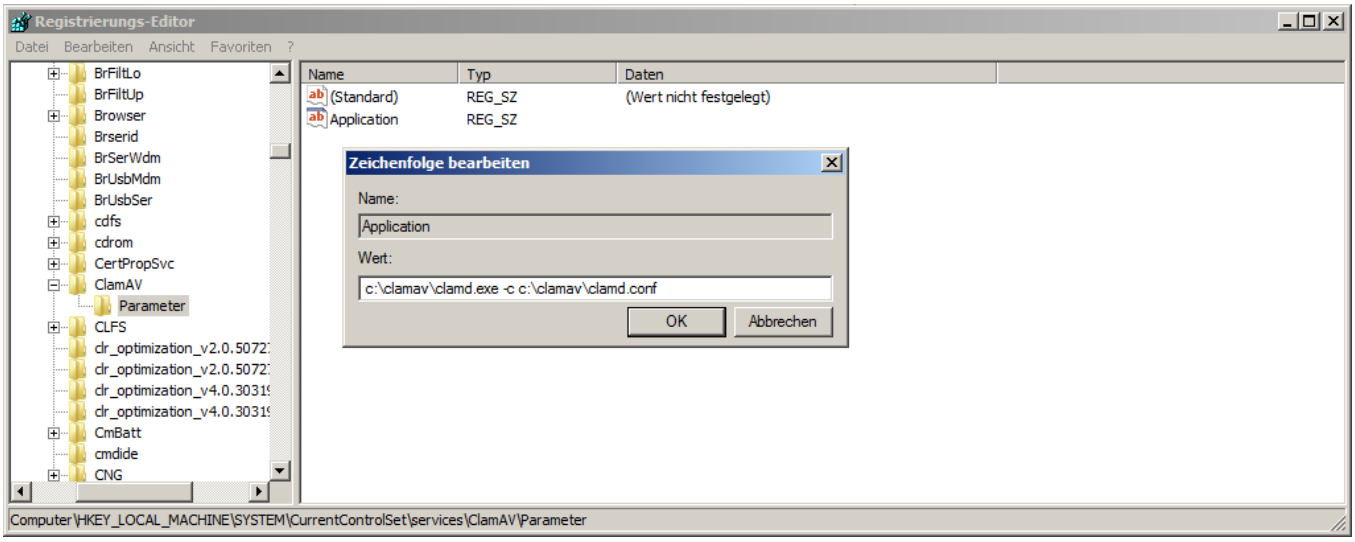
Add a new key with the name: Parameter

Figur 23.



Under the new Key (Parameter) a new string(think this is what it is called in English) needs to be added with the name: Application.

Figur 24.



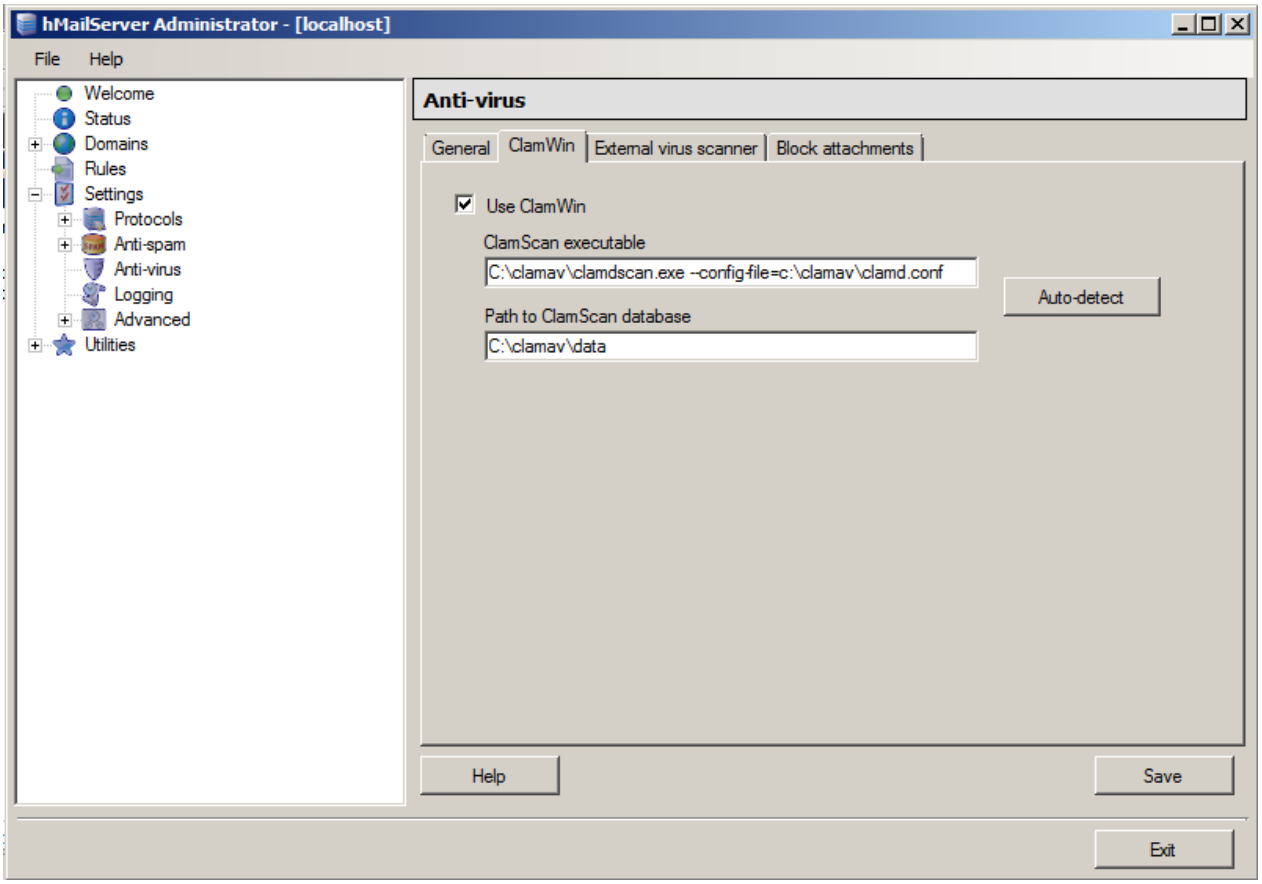
Give the string the value: c:\clamav\clamd.exe -c c:\clamav\clamd.conf

Now the additions to the registry are complete.

Now hMailServer needs to know where the AntiVirus functions are located.

Open hMailServer under settings there is a section called Anti-Virus.

Figure 25.



Under the ClamWIn tab give in the following paths:

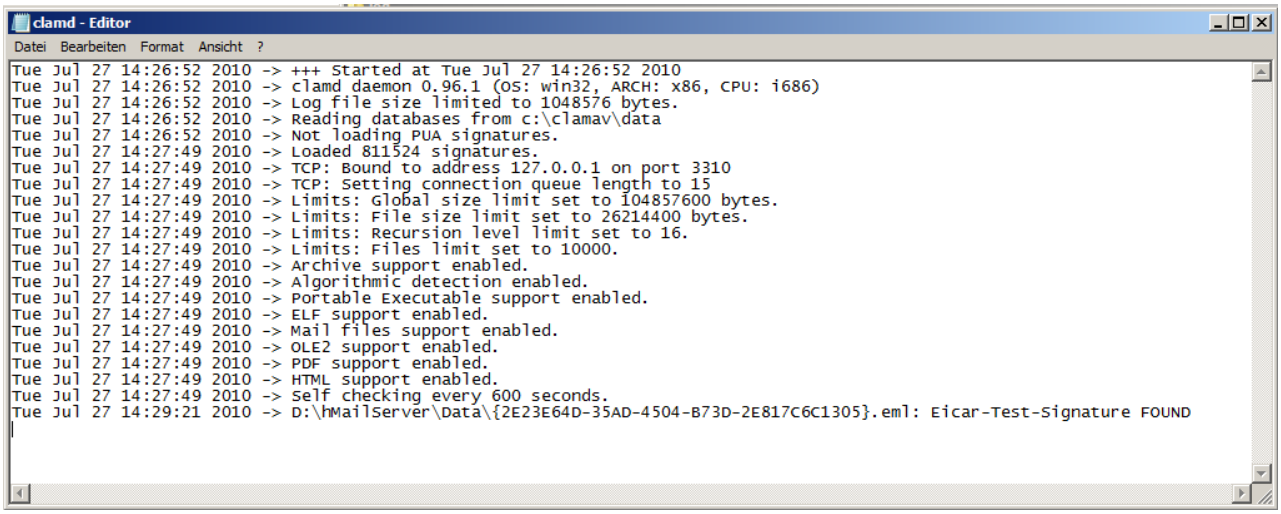
ClamScan executable: C:\clamav\clamdscan.exe --config-file=c:\clamav\clamd.conf

Path to ClamScan database: C:\clamav\data

<Save>

Now the AntiVirus needs to be tested to see if it works. Using a real virus is too risky so we are going to use the Eicar test virus. Download the Eicar test virus from the internet and send it from one hMailServer account to another. The email should not get through. To see if the scan was successful open the clamd.exe log file (C:\clamav\log)

Figure 26.



The very last line in the log should show that the virus was successfully detected.

The pictures are in German but the locations of each key should be the same so following the pictures should work 99.999% of the time ;).....

And that's that, AntiVirus set up, configured and ready to go. Props should really go to nico aka tbb in the hMailServer forum for making it all available.