ClamAV- GUI for eCS V3.0.0

(c)Remy Dodin

Graphical Interface for ClamAV antivirus tool

Clam AntiVirus° is a GPL anti-virus toolkit for UNIX (and OS/2). The main purpose of this software is the integration with mail servers (attachment scanning). The package provides a flexible and scalable multi-threaded daemon, a command line scanner, and a tool for automatic updating via Internet. The programs are based on a shared library distributed with the Clam AntiVirus package, which you can use with your own software. Most importantly, the virus database is kept up to date. A multithread plugin for InetPowerServer is available, ask for details (not free software).

Table des matières

Overview

ClamAV-GUI for eCS is a friendly interface for OS/2 ported ClamAV anti virus tool. Installation is done through WPI package which is the best and eCs base included installer and installation database. You can run more than one instance and you can drag/drop files or folders on ClamAV-GUI icon for ponctual scan.

Installation

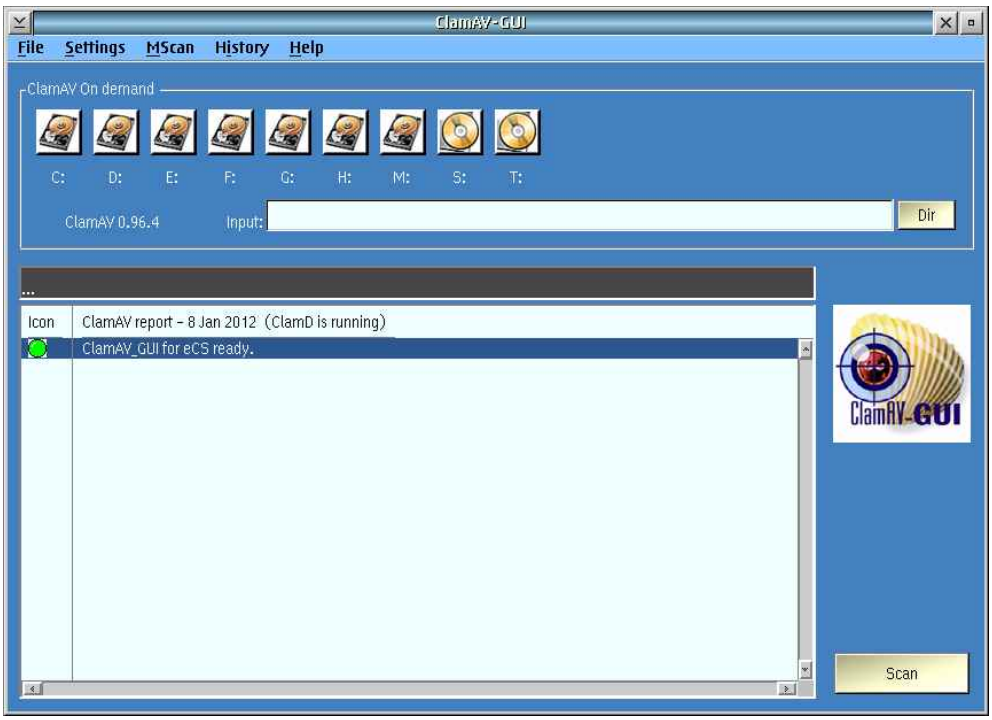
Pre-requisit

- Have an OS/2 or eCS environement (e.g. eCS V2 GA)
- Install required ported ClamAV (WPI or RPM/YUM by Yuri) or my latest ClamAV WPI package anti virus tool before installing ClamAV-GUI for eCS. (If ClamAV was installed using RPM/YUM, see information about RPM checkbox under Settings - ClamAV-GUI must be restarted after RPM/YUM checkbox was checked and before any other settings)
- have pre-requisit for ClamAV ported installed too.

Install process

1. Run ClamAV-GUI WPI package and follow installation. Prefer default suggested installation path
2. At first ClamAV-GUI run, 3 required sub-directories are created and named:
   - Quarantine (any move or copy infected files are placed here if requested)
   - share (used for some temp files and/or virus database signature)
   - Userlist (place any user directory or file to scan list here. Use UCL (User Clam List) extension name

Main windows:



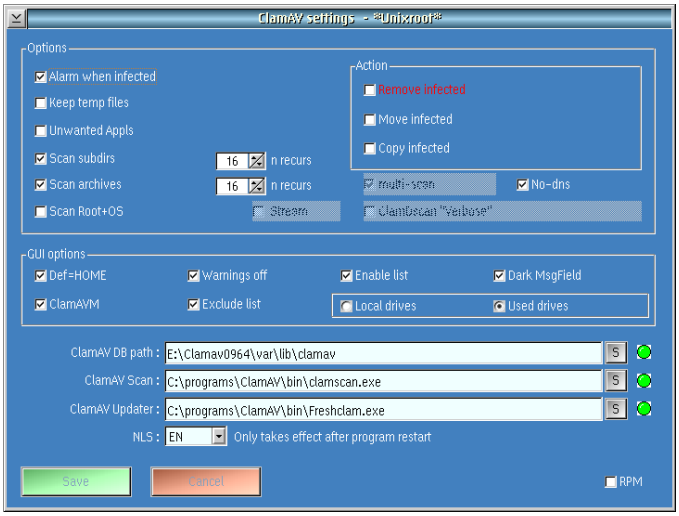
- Drive list allow you to select full drive to scan and set the default drive letter top use for [dir] option
- [dir] open a directory tree view to allow user selected directories to be scanned. It allows to create or recall user created list if the correct option is set under **S**ettings
- ClamAV 0.96.4 (field showing ClamAV version. If this isn't ok, check Settings and verify Clamav.dll is under a valid dll path – If a different clamav.dll build is found than the new one under installation path, a warning message is issued
- Right field is the file/dir input field send for virus scan. Click on drive or dir to add directories or full drive
- Dark grey field is the message field displaying current process (Clamdscan only show defined directories available under the input field.
- Bellow the message field is the report field under which scan result and other action are reported.
- Right col is used to display final report ICON result (ok or infected), current status [running...], [History] or [processes] and the scan button to start the scan.
- Support of background color change using drag/drop color (to resore default color, drop black color in background or go through GUI colors window under settings). At close time, color parameters are saved for reuse for futur run.
- **You may copy rxu.dll from under rxu extra package** under boot_drive:\ecs\dll or boot_drive:\os2\dll if you have some troubles starting ClamAV-GUI (ClamAV-GUI should be able to add extra libpath for the dlls)

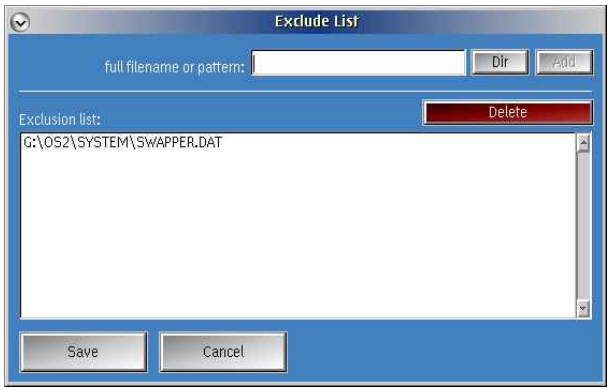
Note: A drag/drop of files or directories onto the ClamAV-GUI icon starts the scan immediatly as single run process providing single file or directory name as paramters does the same.
Any subdirectory added as parameter and preceeded by # makes process to use configured recursive dir option.
This facility is used by the scheduler daemon (latest short results infos are keept into INI file)

Clamavgi.ini is under ClamAV-GUI program path but it could use an older ini under ..\OS2 !

Settings

Open Settings and correct default settings if needed (if config.sys includes a « SET UNIXROOT » statement, it appears into parameters title .





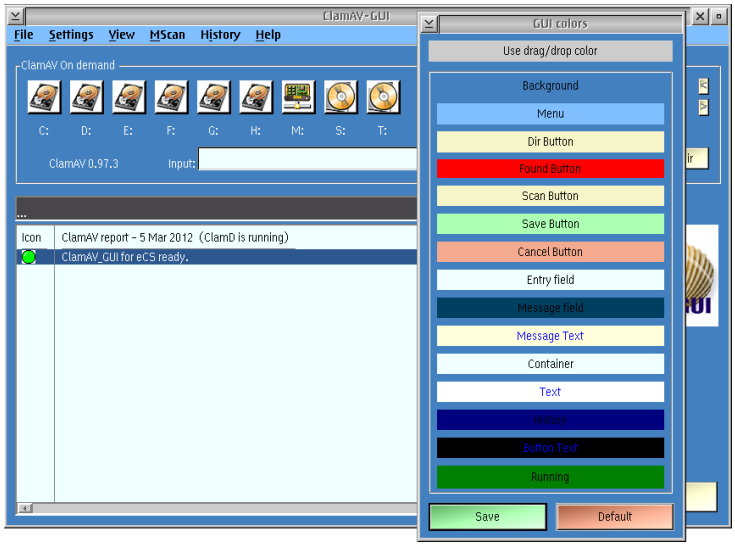
- Alarm on infected (Clamscan and ClamAVGUI parameter to provide a ring tone for found infected fiels)
- all (Check this box beside Alarm setting if alarm should occur on any infected file)
- Keep temp files (Clamscan parameter)
- Unwanted appls (Clamscan parameter. This could provide unwanted alerts)
- Scan subdirs (ClamAV enable subdirs scanning - see [n recurs] for branch level)
- Scan archives (ClamAV enable archives scanning - see [n recurs] for branch level)
- multiscan (Clamdscan parameters usefull on SMP systems. ClamD could crash if no well tunned)
- No-dns (Used by Freshclam to get virus database updates. Older systems or firewall may need it)
- Remove infected (Clamscan will remove an y infected files * be very carefull with this option)
- Move infected (Clamscan will move infected file to « Quarantine » folder)
- Copy infected (Clamscan will copy infected file to « Quarantine » folder)

- Def=Home (Scan HOME dir as specified into config.sys when no specified exist into the input field)
- Warnings off (removes any warning/excluded file messages from ClamAVGUI report panel)
- Enable list (Enable option to save and call back user directories/files generated list for scan)
- Dark MsgField (set reverse video color for ClamAVGUI message field)
- CalmAVM (Auto-Start ClamAVM – rxu.dll required to have ClamAVM running)
- Excludelist (Create a scan exclude list for Clamscan and/or Clamd including, files, directories or text string) * Updated in V3 (enable checkbox under exclude dialog for use with clamd)
- ClamAV Dbpath (specify fullpath to ClamAV database files – use fileprompt button and select « main.cvd or main.cld »)
- ClamAV scan (specifiy used program name for scanning process. It could be Clamscan or Clamdscan or any ClamD client able to provide same messages as Clamdscan or clamscan.
- ClamAV Updater (specify Freshclam program to update ClamAV virus signature databases)
- NLS (EN/FR/DE are currently supported but you can create your lng file)
- ClamDscan **« Verbose »** Run ClamDscan using an input file to get Scanning file listed into dialog as well as enabled « Stop » button - * Updated in V3 (added moving wait info for long scan wait)
- - priority Enable/disable lowering scan process priority (first value could be **0** 'idle', **1** 'normal' ***2*** *'high' (do not use this value)* while last number is the idle value in the range from 0 to 31)
- RPM (experimental option to use if ClamAV was installed using RPM/YUM)

Note: RPM option wasn't tested due RPM/YUM isn't operational and my system incompatible but End users helped me making it well running. Thanks to them
When using ClamDscan or starting Clamd first ime, If original file is found, it is suggested to choice between the configured ClamAV-GUI provided config file or the original file which may not work as is.
When adding Clamd into the config.sys, initialization process makes it not usable with Clamdscan and message no connection is returned. Use Clamscan as « engine » or start ClamD from the startup folder or from startup.cmd

Color settings

Extented color « drag/drop mode only » added since 1.6.0 through a new window. Colore are saved without restart



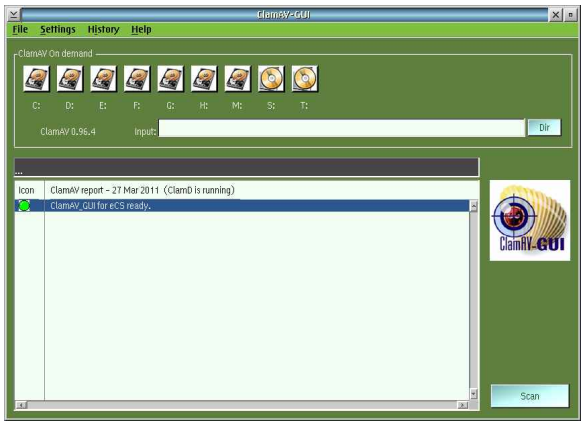
Some build-in themes exist. To apply one of them, select the new theme from under « View » option from menu bar and ClamAVGUI will restart using selection. To reset colors to defaultvalue, click on [Default] under colors settings.

[Dir] window options follow

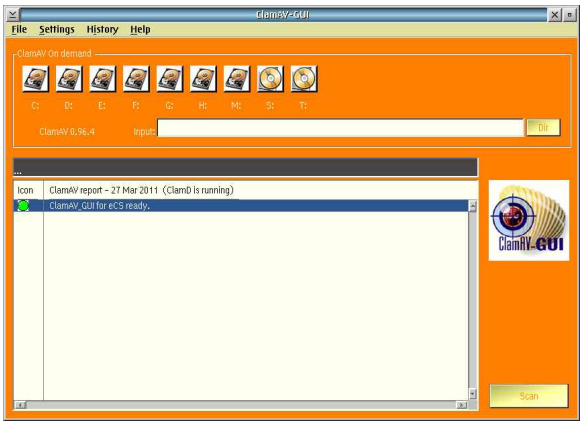
Color preset (Menu option « View »)

blue (see above picture)

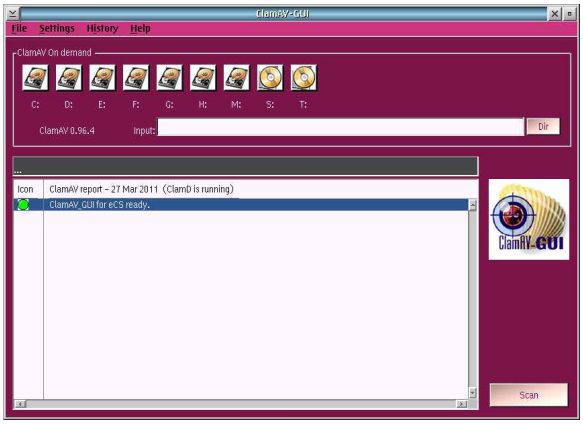
green_kaki



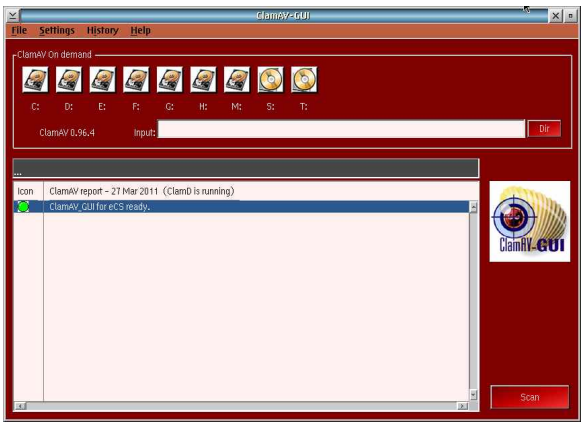
orange



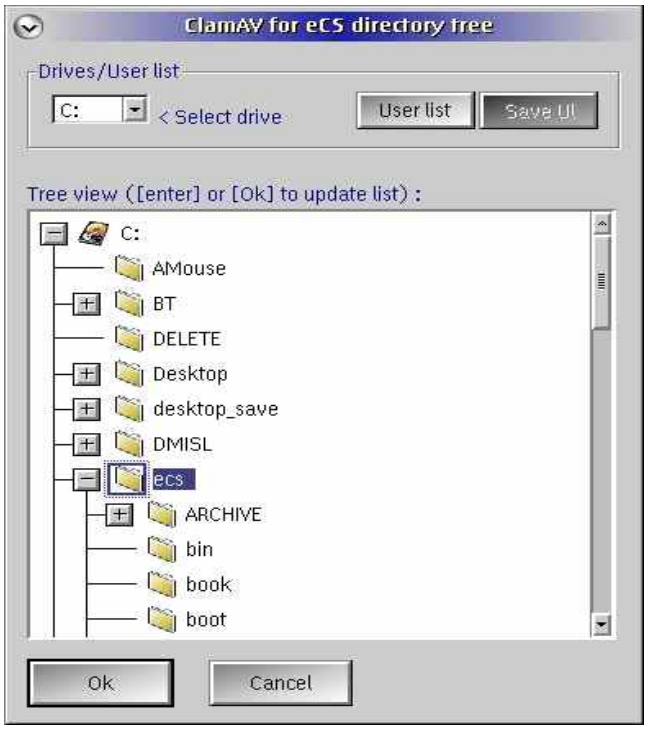
purple



red



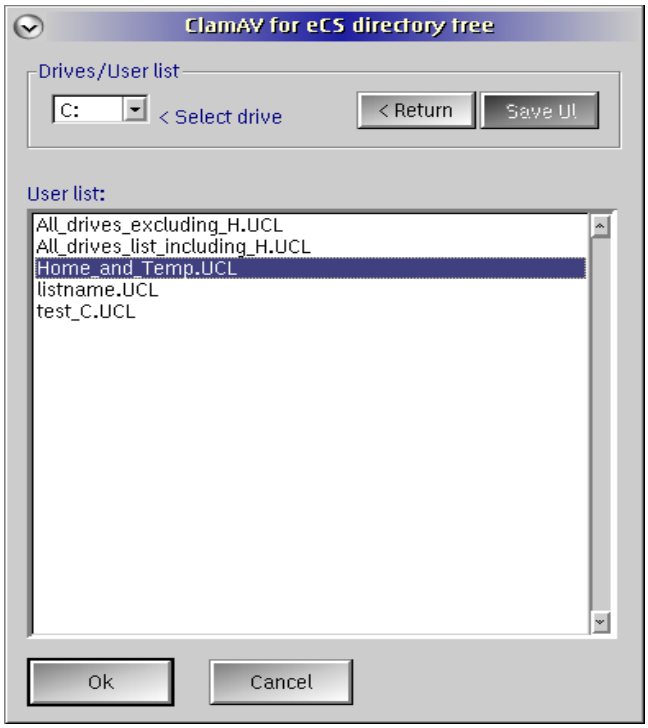
Path selection



To add a new directory into the scan list input field (on main menu)

1. Select a directory and click two times on it or enter then repeat the operation until all required directories have been added.
2. Select a directory and click on [Ok] to add it into the scan list and close [Dir] window
3. A green led (bottom right) flashes as soon as the selected entry is successfully added into the « input field »

Create / Use user scanlist



Click on **[User list]** to view all user saved scanlists.
To create a new list, add all required directories or « files » if manualy
added into the input field as quoted entry
e.g. "C:\HOME\DEFAULT\TEST.TXT'

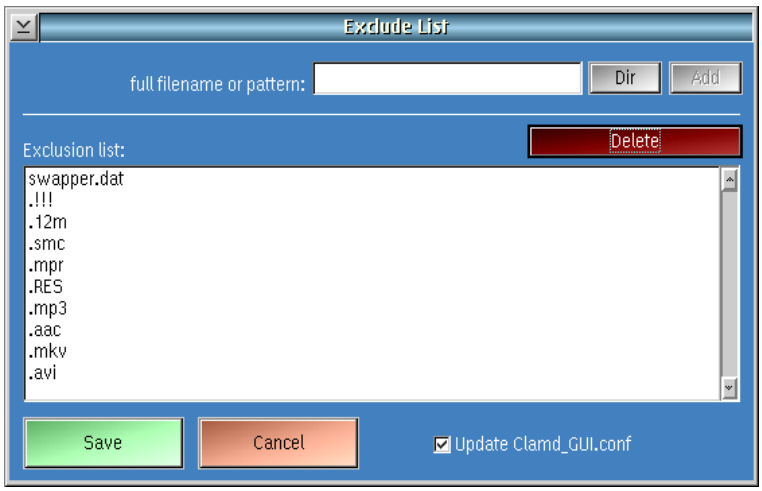
The contain from the input field will be save into a user named file of UCL type.

To use a User list as input scan field, enter on the the selected list or select
and clik ok.

Note : **Created User list are elligible for ClamAVM** (monitor/scheduler) program

Click on **[< Return]** to go back to « Tree view »

Use of exclude list

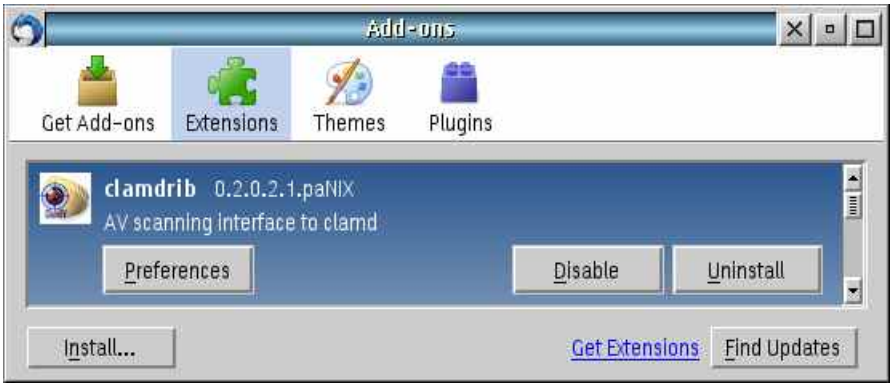


Enter any patern or full filename corresponding to files or path not to be scanned. You can use entries like in the picture at left side of this text.

Enable Update Clamd_GUI.conf file for use with ClamD / Clamdscan (I would suggested to check under internet or clamd.conf man file about how to specify paterns)

Install updated Clamrib Add-on into thunderbird *(tested with ClamAV 0.97.3)*

Open thunderbird and Tools => Add-ons

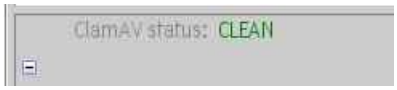


Click on Install... and select the clamarib xpi file under ClamAV-GUI program path

After installation, restart thunderbird and return into add-ons. Proceed to a test. Click on Preference and Test settings

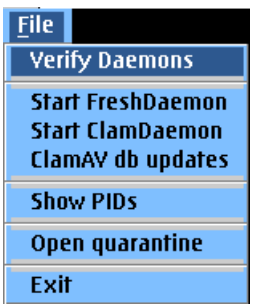
3if it is ok, you should get ClamAV returned installed version »

Under Thunderbird mailbox, you'll have a ClamAV enabled icon and each incomming scanned email will have a scan status hopefully « **CLEAN** »



Note: If the scan fail on attached files above 1MB under single core process, disable the add-on

ClamAV-GUI Menu bar

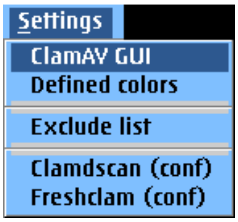


« Files » options:

1. Verify Daemons : Check if Daemons are running and enable/disable corresponding options
2. Start FreshDaemon : Start Freshclam as daemon which is used for auto virus database update (default setting when started from ClamAVGUI = 2 times per day
3. Start ClamDaemon : Start Clamd for system protection
4. ClamAV db update : Start Freshclam to update virus database on-demand
5. Show PIDs : Enabled if rxu.dll is found under .\ecs\dll or .\os2\dll and list all running processes elligible for a « try to kill » because no garanty

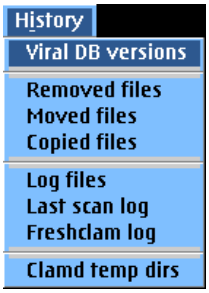
is given about succeffull kill. e.g. Use this option to stop ClamD

6. Open quarantine : Open quanrantine folder to check « moved/copied infected files »



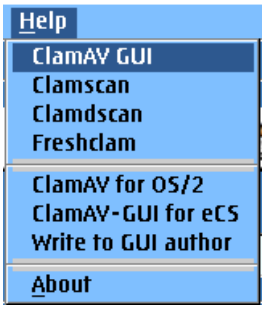
« Settings » options:

1. ClamAVGUI : GUI and ClamAV settings
2. Defined colors : Cutomize ClamAVGUI background/foreground colors
3. Exclude list : Define an exclude list for Clamscan
4. Clamdscan : Edit Clamd.conf or Clamd_GUI.conf config file
5. Freshclam : Edit Freshclam.Conf or Freshclam_GUI.conf config file



« History » options:

1. Viral DB versions : Last on-demand freshclam virus database update date and time and corresponding main and daily virus databases versions
2. Removed files : Allow you to review successfully removed infected files history
3. Moved files : Allow you to review successfully moved infected files history
4. Copied files : Allow you to review successfully copied infected files history
   note: Green icon for Removed entries and Yellow for others
5. Log files : « manage », view and/or deleted clamscan or clamdscan log files
   Green icon for current clean scan log or red icon for logs having « FOUND » files
6. Last scan log : « browse » last log file (now in the report container) – RMB popup enabled
7. Freshclam log : Show freshclam log file from default ClamAVGUI setting
8. Clamd temp dirs : Clamdscan requesting scan to clamd (daemon) creates temporary directories and files. Use this option to view and/or delete unwanted temp directories



« Help » options:

1. ClamAVGUI : Very short help message
2. Clamscan : Opens Clamscan html web pages
3. Clamdscan : Opens Clamdscan html web pages
4. Freshclam : Opens Freshclam html web pages
5. ClamAV for OS/2 : Yuri's WIKI link
6. ClamAV-GUI for... : My ClamAV-GUI web page for updates review if needed
7. Write to GUI author : Send me an email (open your email program)
8. About : Copyright and programs version

Mscan Menu item : Run a Memory loaded files scan

View

*** New V3** This new menu entry allow you to refresh listed drives useful when you plugin a new USB key or disk.
Older presets command files are now all replaced by build-in option with au-restart for easy to use.

History entries

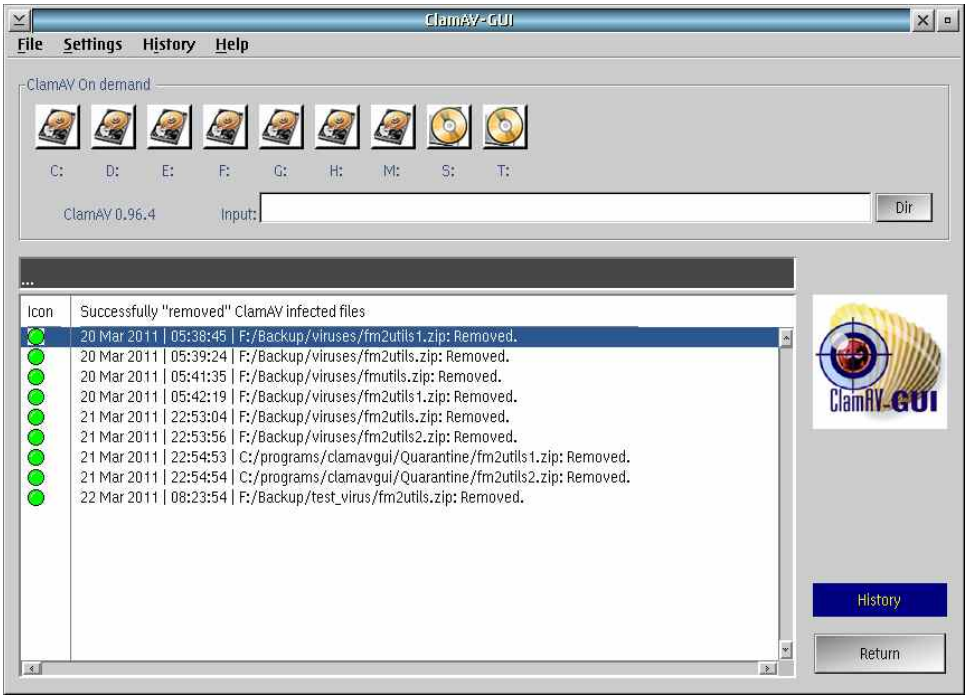
Viral DB version

Display virus database definition files updates (this entry is updated after each « Refresh » action done from ClamAV-GUI. * New (now, display show full db updates details using sigtools as well last date/time)

Removed files

Display history of successfully **removed infected files**. This is a cumulative log.

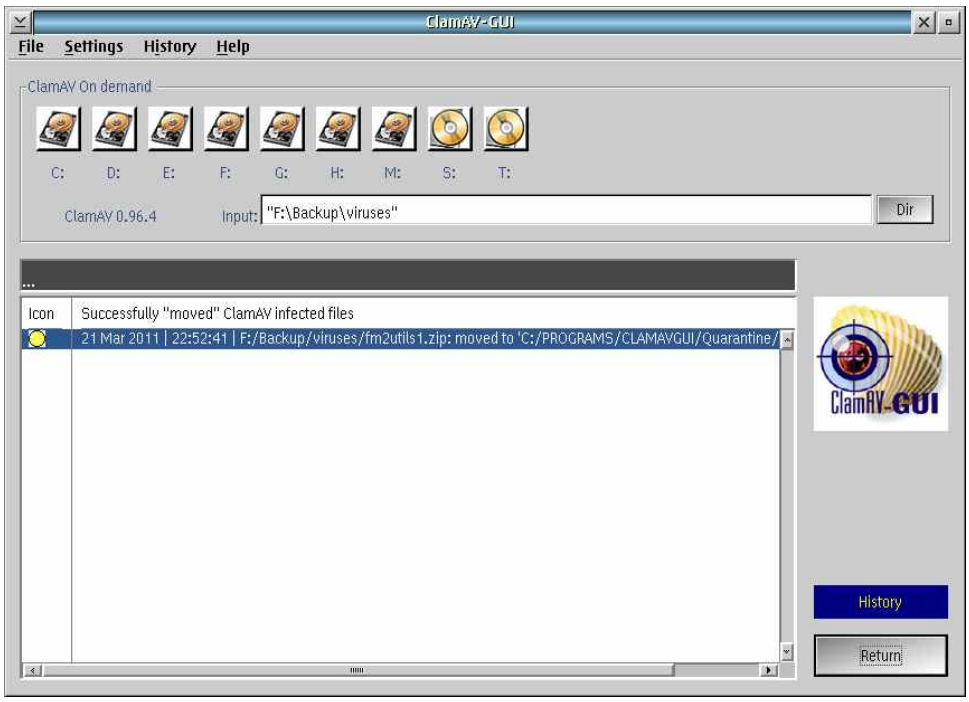
All entries are préfixed by the the logdate and logtimeAs you can see, a green icon is displayed telling you this file no more exist. Click on return to go out of this display.



Moved files

Display history of moved infected files into « quarantine » folder. This is a cumulative log

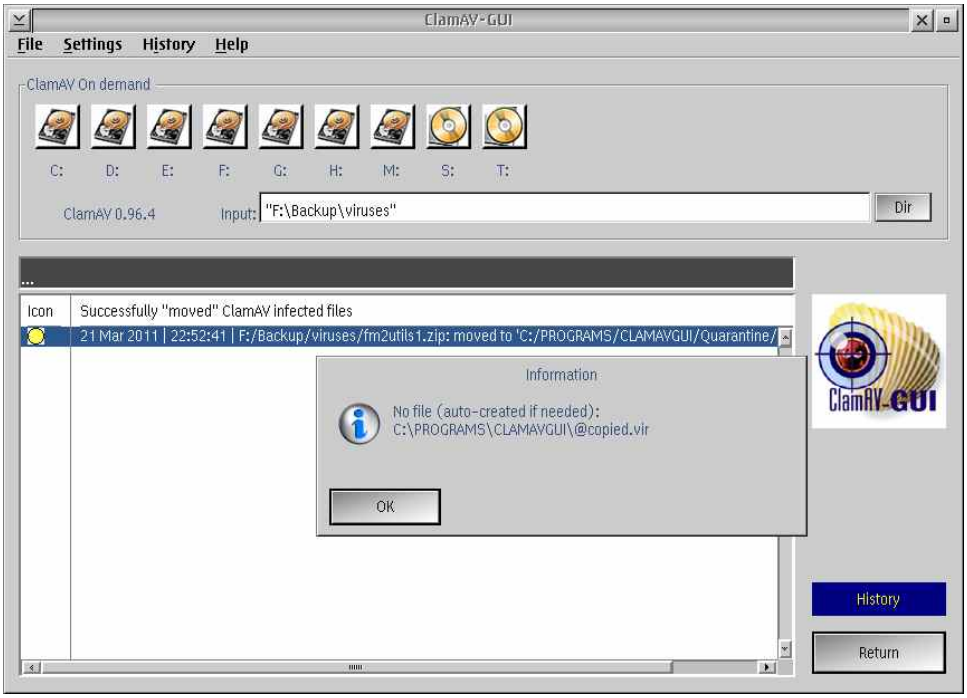
All entries are préfixed by the logdate and logtime.



As you can see, a yellow icon is displayed telling you this file wasn't deleted and could be recovered.

Copied files

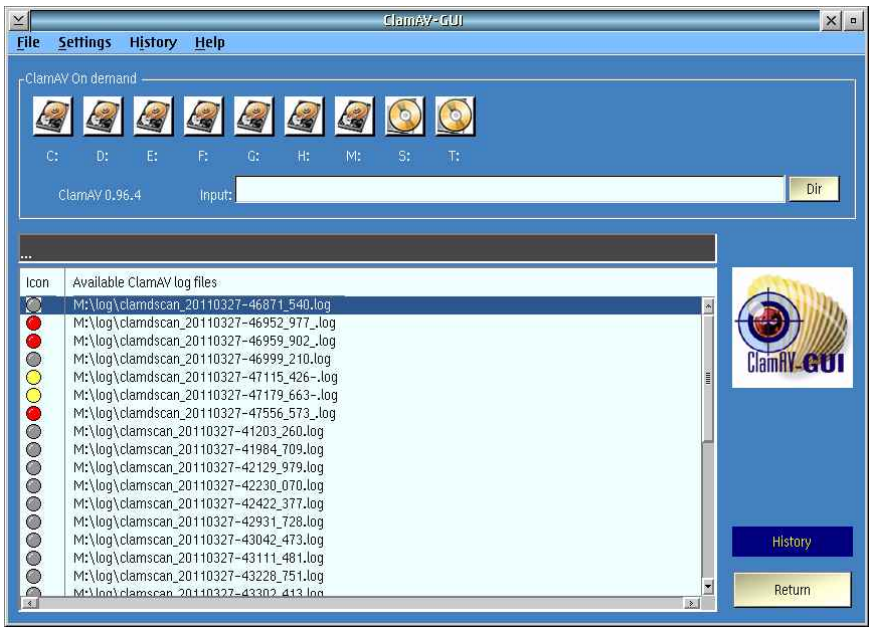
Display history of copied infected files into « quarantine » folder. This is a cumulative log



All entries are préfixed by the logdate and logtime. As for « moved » option, displayed icons are yellow. When no « copied » operation was logged, above message is displayed.

Log files

Display all Clamscan or Clamdscan log files available under log path.

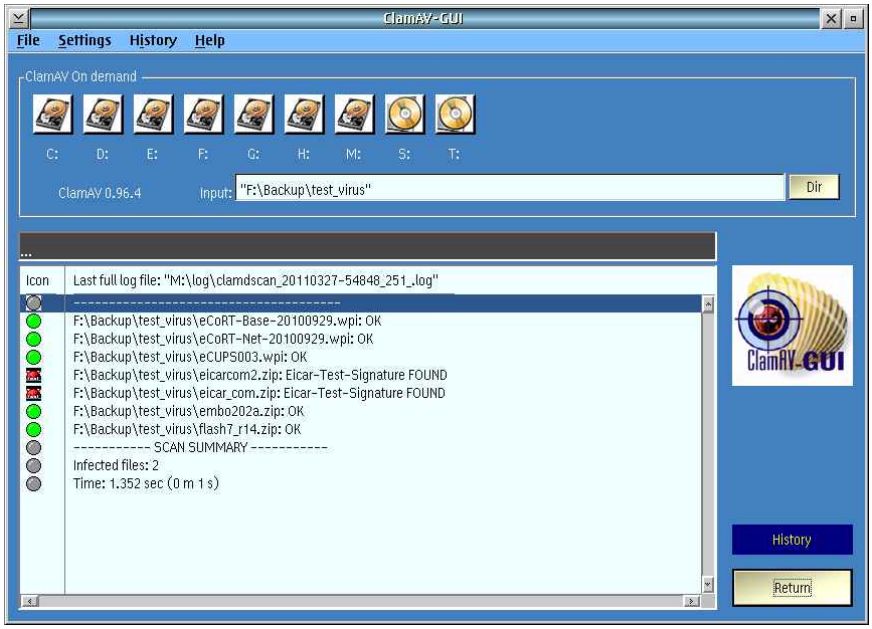


Any log file having infected « FOUND » entries appears with a RED icon (only for log files generated under ClamAV-GUI v2.2.0 or above). Entries having a yellow icon are for log files of user stopped scan. Each filename is composed with the type of scanner user and the date/time of the scan.

A green icon is only used the the current scanlog result when no infected file was found.

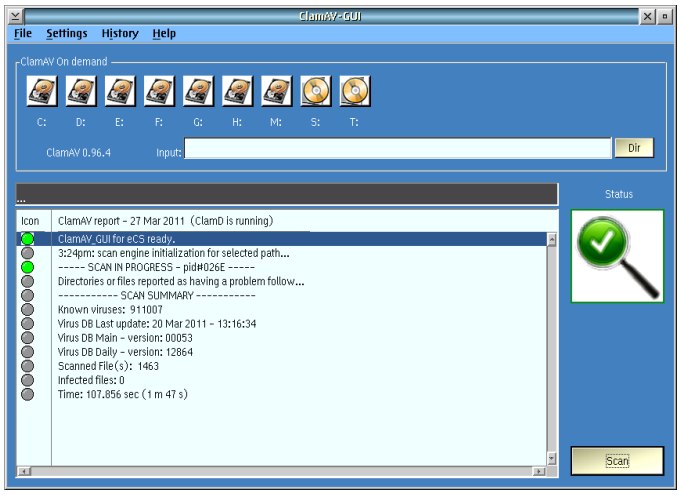
You can use RMB (Right Mouse Button) and select « View » (to display the log contain with status icon like it does when using **« Last log scan »**) or « Delete » selected log files.

Last log scan

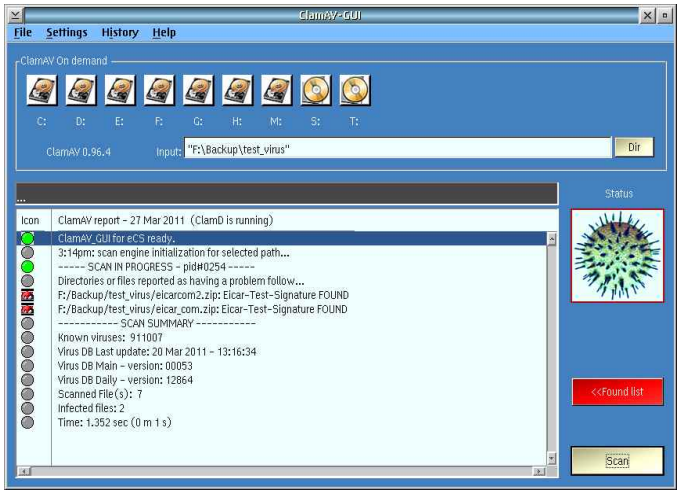


Any entries file entry not having « FOUND » has a green icon, any text entry has an information icon while infected files have a viral icon. Delete will deleted the file from the disk but it doesn't remove the entry from the existing log.

Successfull scan result

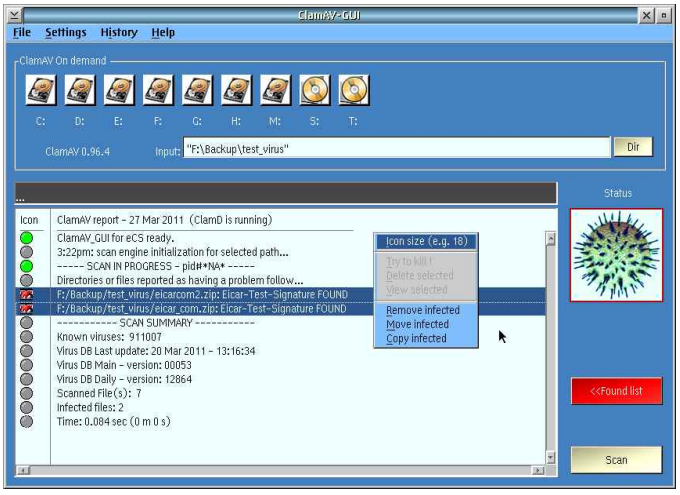


Virus found during clamscan/Clamdscan



* New (v3)
I message about number of detected infected files is now displaied.

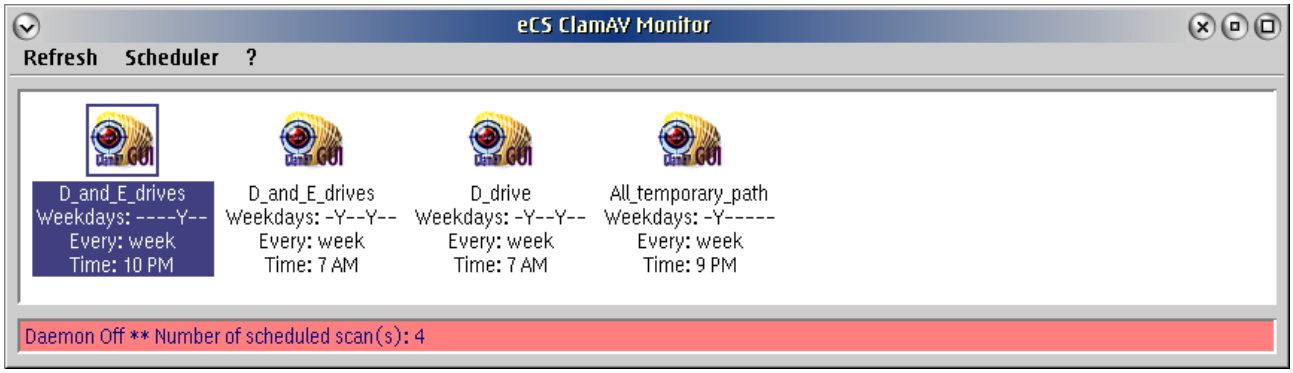
Infected file removal on demand request



ClamAVM for eCS 0.1.2

ClamAVM is a monitoring/scheduler tool. It allow you to stop running scan started from ClamAVGUI and mostly using clamscan. This is an experimental build but the ClamAVM should be ready enough for a all day use except ClamSCD which isn't deep tested (ClamSCD didn't save already executed scan at close time)

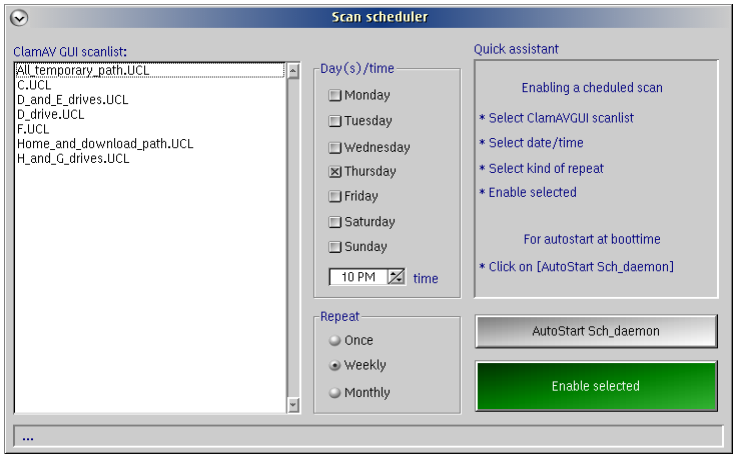
Only one instance of ClamAVM can be running. If you set « ClamAVM » option under ClamAVGUI and start more than one clamavgui instance, only one ClamAVM will be started. Since 0.1.0, ClamAVM works now in auto-refresh mode.



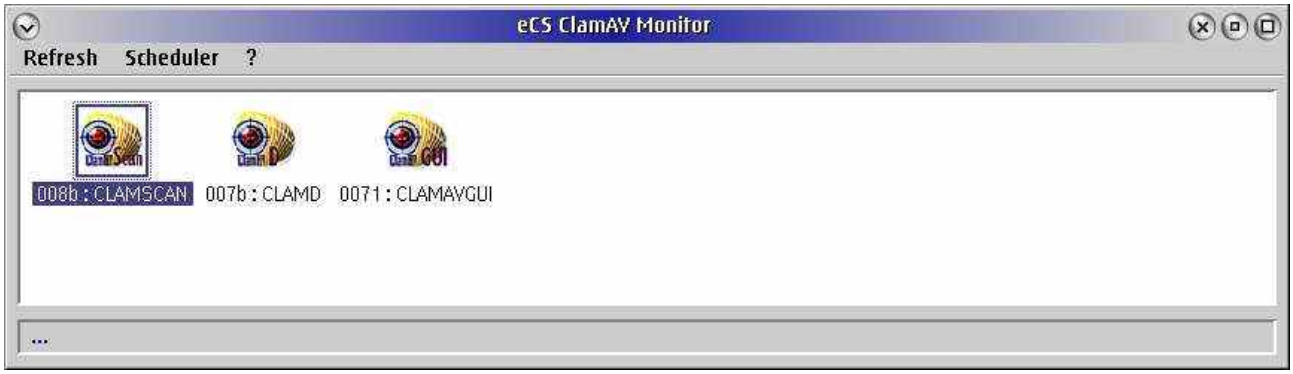
This is how scheduled scan are listed into ClamAVM. You can delete any and/or create new scheduled scan from scheduler barmenu.

Note: ClamAVM wasn't a lot developped yet and it is planned more corrections/improvements in the futur.

Defining a new scheduled scan entry:



Select a scanlist to be submitted at scheduled scan. List are created unde ClamAVGUI, select running days and running time and at least, the process repeat time e.g. Weekly
Once you press on Enable selected, value is saved into ClamAVGUI ini file and usable for ClamSCD (the scheduler daemon)



Any click on Refresh show again updated Clam* processes which can be stopped using popupmenu from RMB (Right Mouse Button).

Note: ClamAVM uses background color defined under ClamAVGUI
This GUI program is distributed in the hope that it will be usefull but WITHOUT ANY WARRANTLY. Please read general terms and conditions

These both user interfaces are free to use exclusively under eCS. It is a freeware interface and it is forbitten to include it into any commercial product without explicite author autorization.

Special agreement is given to eComStation for a free integration in eCS V2 as addon.

General terms and conditions for freeware producs / GUI

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMA4 NCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

END OF TERMS AND CONDITIONS

Rémy DODIN