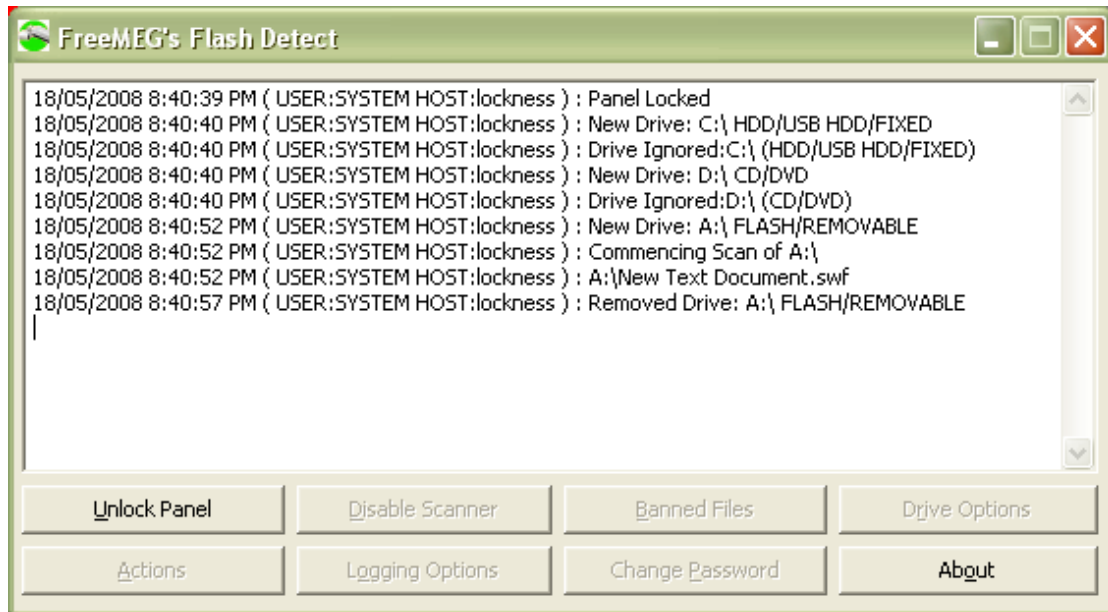


!! ~~ FlashDetect ~~ !!

[By FreeMEG Software](#)

File Detection, Lesson Protection, Bad Student Correction. Your friend against all digital odds!



So what does it do?

FlashDetect sits happily in the background running as either a system service or as an interactive application. It will then continuously monitor for new disks/usb's or CDs that are placed into the computer. It will then process the contents of these against a predetermined list of bad files and if it finds them it will continue to dish out some punishment to that user.

So what kind of drives can I monitor?

Any drive really that windows can understand. But to summarise:

- A) Floppy Disks, USB's, ZIP's, LS120s, and other Removable Disks
- B) Harddisks, USB Harddisks and other Disks considered fixed
- C) CD-ROMS, DVD-ROMS, and Other Optical Drives
- D) Network Drives/Remote Drives

You can choose in the setup what drives you would like to monitor or ignore.

So what kind of punishment does this dish out?

There are 6 options, each a little worse than the previous. Finally! an Application worth the administrators time to configure! Anyhow here is a table summarising:

Action	Elaboration	User Annoyance
Just Record in Log	Often for the system administrator who is new to the job and doesn't want to tread on too many toes. This will just log what this naughty user is up to. That is if logging is even enabled.	They probably won't even notice. Which is good, because you can collect all sorts of data to take to the Principal later and bust them big time.
Display a vibrant but intimidating message on the screen.	A very flashy and audible screen will take over their desktop, and they won't be able to do any work until they remove those suspicious files. Just to add to the embarrassment, the message stays up on the screen for a certain amount of time (defined by you) after they remove the files.	Shocked if anything, they probably get laughed at by other students and attract the kind of attention that would make the classroom teacher suspect something is up.
Silently Prevent Access to the files	So if you are the kind of administrator who likes to pull the legs of spiders, you will probably like this option. With them knowing it will lock all the files so they cannot be opened from the disk. Oh and they can't be erased either by the user.	Just sit back and laugh as those students try to play their flash games and instead get a big stinking error or even better a blank browser window. At this stage you are definitely starting to annoy the end user.
Silently Delete the files	This is so badass!! To quote the language from the Y generation. So! They don't even know it, but when they put their disk in the drive, Bang! Their bad files are gone!	This one will give you the administrator probably the most satisfaction. But beware, those students may be so annoyed they will actually talk to their parents, and prod them to complain. So scrub up on your knowledge of the Computer Acceptable Use policy, you may need to fallback to it.
Alert User, offer grace period to remove files/device, delete files	Okay this is hard to summarise in a small dialogue box. But, it basically has the same outcome as the silently 'delete the files' option except it gives the student to be nice and redeem	Sort of a mixture of shock, intimidation and annoyance. You'd basically hope they'd be totally confused and in the time it takes for them to drum up the courage to ask a teacher what to do, its

	themselves. A screen similar to the intimidating option appears, with a countdown timer. If they don't comply in the time shown. Bang! Then their files are gone.	two late.
Force Logoff User	Zero Tolerance here. This is sending the clear message of get out of the lab if you ain't working. No grace, no message, just sheer logoff.	Mainly Confusion here, step back and laugh at how many times a student will repeat the process before they realise it might have something to do with the files on their disk.

These bad file lists how do they work?

Well, if you know what *.SWF means and/or maybe *thisfile* then you're 100% there to understanding it.

Okay so every file has an extension and this program allow your to keep a list of them. For example Shockwave Flash Games (most likely thing you want to block) have files with the extension *.SWF. So you add that to the list, then all files that have the SWF will be detected. Now for some reason you may only want the Shockwave games that start with N to be detected, well you could stipulate N*.SWF in the bad files list and wallah!

Now what ever you do, don't do *.* For starters you'll probably axe your systems performance and secondly you could prevent access to all files or worse delete them.

So what are the system Requirements?

Well any computer than runs Windows 2000/XP and maybe Vista (I haven't tested vista). Oh and I haven't tested in 64-bit windows.

You will need some harddisk space: A whole of 2MB hope it doesn't kill the build. And it does use some memory: Anywhere from 4MB to 30MB depending on how many bad files it finds.

Is there any limitations I should know about?

Try to avoid scanning the main SYSTEM harddisks.. It will do it, but it will drag your system into the ground.

Oh and if you choose to prevent access to files, note this thing can only stop up to 65536 files from being accessed.. I know, if only I could make it prevent access to 65537, but that would probably take another 100MB of RAM. If you love swap files or are a little crazy, email me and I can give you a special version that will do 4,000,000,000+ file prevention.

Okay I'm ready to install now!

Well that's great, your not on your own. This program is fairly simple to install but its best to follow the instructions below if its your first time. Now if it's your first day as an IT administrator well.. I'd suggest some familiarisation with your IT environment first because there are quicker ways to get this deployed. Below I'm only going to cover how to install it onto a single computer that you happen to be in front of.

But first.. To System Service or Not To System Service

This program runs either as a system service or just a interactive application. In layman's terms this defines how the program is run, and how rock solid and unbreakable it is while its running. The table summaries the pros and cons of both.

Interactive Application Mode	System Service Mode
<p>Pro's</p> <p>Very easy to install – Well you double click the executable or put it somewhere so it will auto start when the user logs on.</p> <p>Can be centrally managed. – You could sit the FlashDetect files on a centrally accessible network share and easily update the config file</p> <p>Easy to deploy – Run it from a login script in a matter of minutes.</p>	<p>Pro's</p> <p>Secure – Users cannot stop or terminate the application.</p> <p>Loads instantly for all users – As soon as they logon it is available, often before even the explorer user shell loads. Meaning those sneaky users who will try to bypass this program probably won't be able to.</p> <p>Runs anywhere – Because its local, you can send it out on laptops that are no longer connected to the network, confidently knowing those bad files are not being accessed.</p>
<p>Con's</p> <p>It runs with the same security rights as the user – If you choose to save the logs to a network drive, well the user must have write access to them.</p> <p>Users can terminate the application – simply by loading the task manager, selecting the app and clicking end task.</p>	<p>Con's</p> <p>Deployment – Well it's a little tricker. You either have to go to each machine and install it after pre configuring your settings or take advantage of some sort of group policy or start up script. Which requires a little knowledge of Systems Administration.</p> <p>Hard to change settings – Because a system service runs locally, the configuration also sits locally on the machine. To make a quick change to the bad list may require a complex arrangement of scripts made by a smart system administrator.</p>

Personally I like the system service option, but that's only because I don't like smart but naughty students working out how to get around things. In a system service there is not a chance they are stuck.

Installation Instructions

Step 1) Copy the files somewhere

Besides this readme there are a few other files that came in the package. Copy all of them into a folder located somewhere on your computer or network. If it's a system service then it has to be locally, preferably in a folder that sits inside the Program Files folder. I'll give an example:

C:\Program Files\FreeMEG Software\FlashDetect

Now if you are using it centrally on a network well you need to make sure your users can read the contents of the folder. I'd recommend a hidden share:

[\\servername\share\\$\FlashDetect](#)

Shares with a dollar sign can't be seen in network neighbourhood or when you browse the shares of a server. Sneaky hey!!!

Step 2) Setup the configuration

This is a big step and may require you to look in the final section of this document. At a fundamental level you need to run flashtray.exe just once and go through all the menus and select the options that best fit your network environment. More importantly you will want to set the password in the change password menu. This means in future the tray is locked, cannot be closed and the detection program cannot be manipulated or stopped.

Anyhow the program will create a flashdetect.ini file this needs to accompany the flashtray.exe where ever you choose to put it. Note your users will need to at minimum access this to read this file.

Step 3) Setup the program to start when a user is logged on

Service Mode

Make sure you are the type of Administrator who can add system services to your computer. This is nearly all administrators, but in large environments may be different.

Run the installsvc.bat file that is located in the same folder as flashdetect.exe. Oh and make sure flashtray.exe and flashdetect.ini are in the same folder.

Now you can check your system services list which is in **Control Panel -> Administrative Tools -> Services**

You should have in the list a service that is called “Flash Drive File Detection and Removal”

Double click this to get the properties up and check the following settings:

General Tab

Startup type is set to Automatic

Log On

Log on as: Local System Account

Allow Service to interact with desktop is Ticked

And that’s it, next time you start your computer it will run the program upon logon.

Interactive Desktop Mode.

Okay, so run FlashTray.exe from your shared folder on the network or where you chose to put it. Make sure flashdetect.ini is in the same folder.

Places you might like to run flashtray.exe from:

A shortcut placed in **C:\DOCUMENTS AND SETTINGS\ALL USERS\START MENU\PROGRAMS\STARTUP**

An entry in the registry located at

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

A group policy logon script.

A network logon script. (Netware Logon Script/Windows NetLogon)

Using the Program

Once the program loads it sits in the system tray:



FlashDetect is the green icon on the far left.

The icon can actually look like a few different things



When it looks like this, then the program is detecting and everything is groovy



When it is in this mode it means the user has inserted a disk and its scanning the contents looking for those bad files

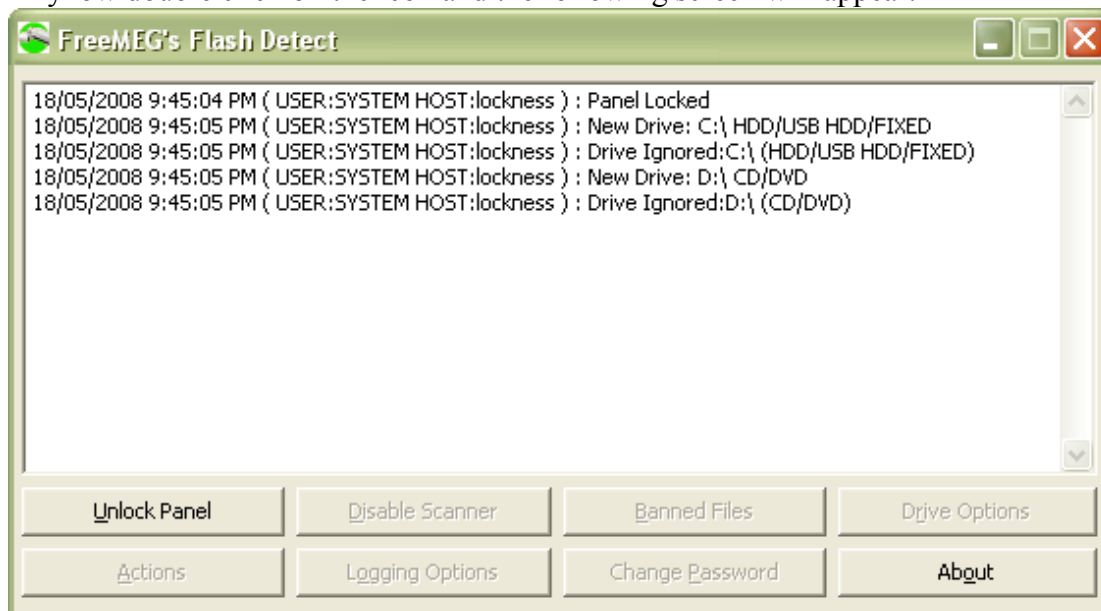


When it is in this mode it means it has found some bad files and is taking the appropriate action that you as the administrator have set.



When it is in this mode it means the detector and scanner are disabled. This mode mainly occurs when you as the administrator have unlocked the panel and have clicked on Disable Scanner button. But users may see this briefly upon logout or system shutdown.

Anyhow double click on the icon and the following screen will appear:

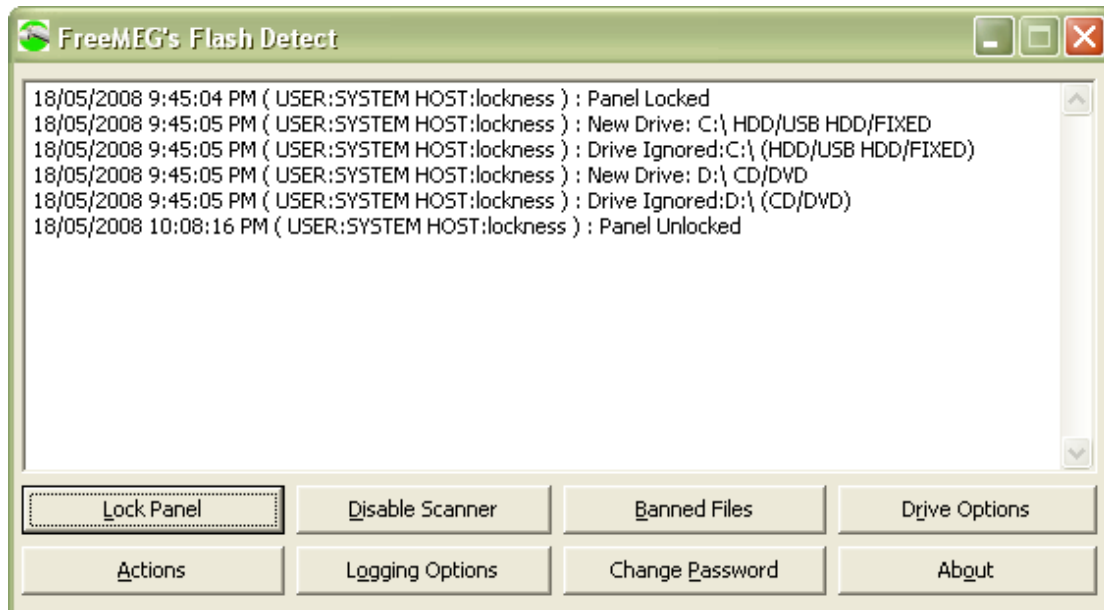


By default if you have set a password, the control panel is locked. There is a log that is displayed on the screen and an about box, to the standard user that's about it.

If you are an administrator you can unlock the panel by entering the correct password:



Note: The log will keep track of failed attempts. More on this in the configuration section at the end.



That's better now we have way more options:

Lock Panel just takes you back to what a standard user sees.

Disable Scanner will disable the detector and scanner. If you want to exit the program properly, you must disable the scanner before you close the window. Otherwise the program just minimises back to the system tray.

Banned Files – (aka the Bad file list) Okay this is where you set the files that are considered bad by the scanner.

Drive Options – This is where you choose what drives and types of drives are scanned.

Actions – This is where you dish out the consequences should bad files be found.

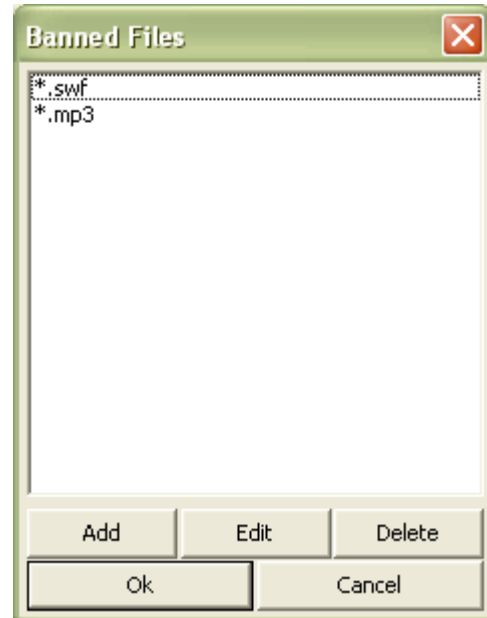
Logging Options – There are a bunch of options pertaining to how the events of the detector/scanner are stored.

Change Password – Change the unlock/admin password here. Setting the password to blank will disable it.

About – Probably the most important button in the program. This allows you to find out more about FreeMEG and this marvellous program.

Configuration Options

Banned Files



Hopefully this screen is self explanatory

Add – Allows you to add a file mask

Edit – Allows you to edit an existing entry in the list

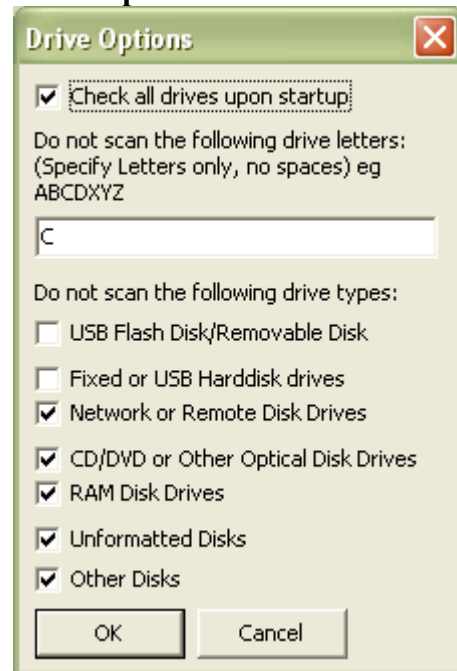
Delete – Allows you to delete an entry

Remember a filemask is a selection of files you do not want those students using so
*.SWF is all the SWF files on a drive. So you need to identify what are bad files, to save time I will suggest some here:

- *.SWF – Flash Games usually, beware some IPT courses may need these
- *.FLA – More flash games, don't forget those IPT courses.
- *.MP3 – Music files probably stuff you won't like too.
- *.WMA – More music files..
- *.M4A – More music files
- *.WMV – Video, probably something silly like a kid hitting his head on a ladder or something
- *.EXE – Executable files, often games sometime viruses. All the exe's a student needs should already be on your network.
- *.BAT – Nasty scripting files that students can use to get around your security. Beware this might actually impose on your network operation
- *.LNK – Shortcuts to other programs, also sometimes a cunning way of gaining access to hidden drives.
- *.JPG – Pictures
- *.GIF – Pictures, might be porn.. do you want porn in your classroom?
- *.BMP – Pictures.

*.COM – More program files of the old fashioned DOS variety. Probably some retro kid trying something low level to gain access to your network.

Drive Options



Here is where you get to define what drives or types of drives are scanned for bad content.

Check all Drives Upon Startup – When this program loads, if this is ticked, it will scan drives that are already in the system. Useful for if that student has already inserted their USB Flash disk prior to logon. Can't see why you would want this off, unless you have some other program that conflicts with this one or vice versa.

Do not scan the following drive letters – Contains a list of letters of drives that will never be scanned or detected. Its good practice to put C in here, afterall that's your system drive right? And you don't want this to be constantly scanned. Goodbye system speed. You may want to put other drives like your network drives, except maybe the students home drive.

Do not scan the following drive types – Okay windows identifies drives and categorises. Ticking any of these will do a blanket ignore on that drive type. Good especially if you are unsure of the drive letters that these devices may use.

Essentially a removable drive is any drive that can be inserted and removed by the user. Eg Flash Drives, USB Pens, Memory Sticks, Compact Flash, SD Cards, Floppy Disks, ZIP's. LS120's. Strangely this does not include USB Hard disks which are becoming popular.

Fixed disks are those that normally are writeable and inside the case of the computer. Hard disks come to mind and that's about it. But don't forget USB Hard disks also fit into this category.

Network disks are mapped drives. No brainer here. You may alternatively know your mapped drives and want to make sure this is not ticked so that you can scan your users home drive.

Optical Drives are those CD/DVD/Bluray drives, normally read-only to the operating system. Remember if you include this type of drive in your scan and detect, the deletion actions won't work and may cause this program to do funny things.

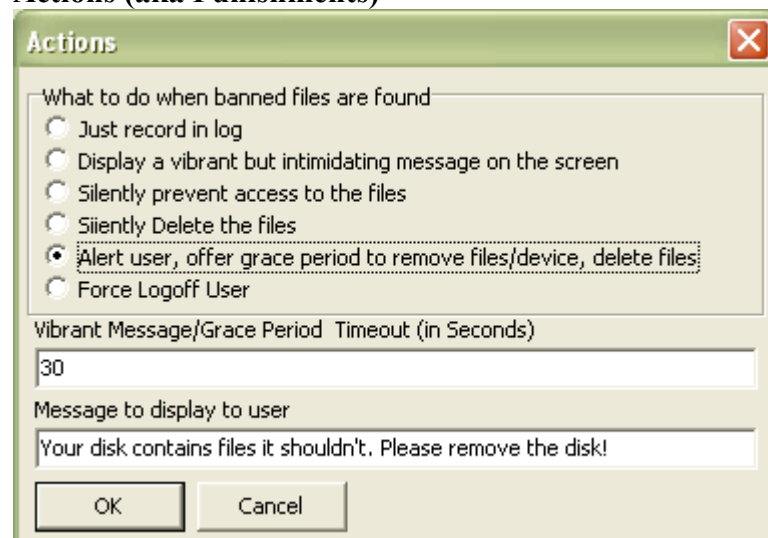
RAM disk drives are drives that are made up of memory that is in your computer. These aren't really used as much as they used to. I just maintained this for backwards compatibility.

Unformatted Disks are any disks that have a file system that is either foreign to Windows or no file system at all. You don't want the detector/scanner trying to access these disks as it will just slow down your computer in its attempt. However if you are crazy or have some underlying operating system driver that may allow access to alternative files systems like MAC HPFS for example, then its work having this unticked.

Other Disks are disks that windows cannot figure out what to do with. Best left ticked, as its probably something really ugly.

These drive types are configured by windows in its API. I just put them here, for compatibility, but usually you can assume the defaults are appropriate.

Actions (aka Punishments)



This is what to do if bad files are found

Just record in log – Will just log the bad files, depending on how the log files are setup.

Display a vibrant but intimidating message on the screen – Until the user removes the files (the disk). This has two options (below) that are important.

Silently Prevent access to the files – Prevents the user from accessing the file by placing an exclusive lock on the file. If they try to access the file they will either get

an error or a blank screen in other programs. They also cannot delete, copy or rename the file. Note: This program can only prevent access to up to 65,536 bad files. So its best not to have a large file list or be monitoring a disk with a large number of bad files like a harddisk.

Silently Delete the files – Instantly deletes the bad files that it finds. Note: If you are monitoring a Optical Drive or a drive that is readonly then this program will not be able to delete the files and will possibly may produce an error.

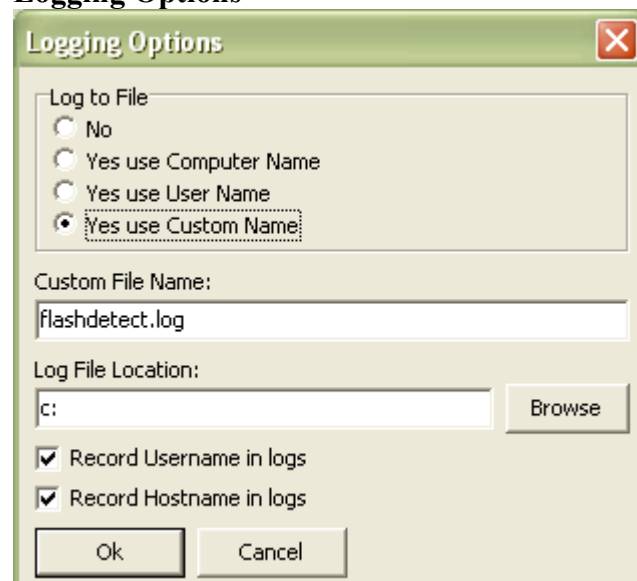
Alert user, offer grace period to remove files/device, delete files – This is the same as **silently delete the files** except it gives the user a grace period by producing an intimidating message on the screen. This has two options (below) that are important. Note: as with the previous option, any bad files found on a readonly drive like a CD or DVD will not be deleted and may possibly cause the program to error.

Force Logoff User – Instantly will log the user off without warning.

Vibrant Message/Grace Period Timeout (in Seconds) – This setting can be used in two modes. A) It can be the number of seconds a user has to remove their files or disk before the program will automatically erase them. B) It is the minimum number of seconds a message will appear on the screen intimidating the user who has placed a disk with bad files into the computer. Once they remove the offending files./disk the message will also stay on the screen for this many seconds.

Message to display to user – When the intimidating screen is displayed to the user a message appears in the centre of it, and this can be customised by you. Try to pick something that is appropriate to the action. For example if you are going to delete the files if they don't remove the disk, then mention this in the message. Or if you want to let them know this will be reported to the principal then mention this here. Really its whatever you like, just as long as it clear. The amount of words in this message is directly related to your screen resolution. But really your only have about 100 characters of space.

Logging Options



The screenshot shows a dialog box titled "Logging Options" with a close button in the top right corner. The dialog is divided into several sections:

- Log to File:** A group box containing four radio buttons: "No", "Yes use Computer Name", "Yes use User Name", and "Yes use Custom Name". The "Yes use Custom Name" option is selected.
- Custom File Name:** A text input field containing the text "flashdetect.log".
- Log File Location:** A text input field containing "c:" and a "Browse" button to its right.
- Checkboxes:** Two checkboxes are checked: "Record Username in logs" and "Record Hostname in logs".
- Buttons:** "Ok" and "Cancel" buttons are located at the bottom of the dialog.

Log to file:

No – This will just log events to that main screen

Yes use computer name – Will create a file with the name of the computer in the location specified below. Useful if your log location is a network.

Yes use user name – Will create a file with the name of the user in the location specified below. Useful if your log location is a network.

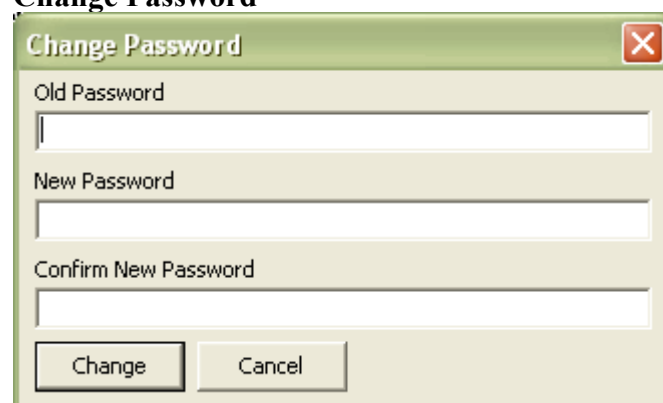
Yes use a custom name – This is used in combination with **custom file name** to set a log file name of your choosing.

Log File Location – You can specify where the log file should be written to here. This is useful if you have a large number of clients and you want them to store all their data in a central network location.

Record username in logs – If ticked then the username will be stored in the log. Useful for auditing in a centralised network log location, or creating an audit trail.

Record hostname in logs – If ticked then the hostname (computername) will be stored in the log. Useful for auditing in a centralised network log location, or creating an audit trail.

Change Password



Will set a password which will lock the panel by default when the application is loaded, and will prevent regular users from accessing the configuration settings or shutting the program down.

Old Password – You need to enter the old password here, to make sure you want to change the password. Note this will be greyed out if no password currently exists.

New Password – What you want the new unlock password to be. Setting this to blank will disable the password.

Confirm New Password – This must be the same as new password for the password changes to go through.

Note: Password are case insensitive. Try to use letters and numbers only. If you stuff up the password, you can delete the **UnlockPassword** entry out of the flashdetect.ini and start all over.

Some final notes about using the Program.

Can't Close the Flash Detection Program

If you are running the program in service mode, and you disable the scanner then close the program, it will automatically load up a new copy. This is because the flashdetect system service (covered earlier in this document) detects that there may have been a hack attempt and therefore starts the application again.

To properly close the program when it runs in service mode, you must actually stop the service. This can be done in two ways:

- a) You can run StopSVC.BAT hopefully located in the same folder as flshdetect.exe
- b) You can stop it in your system services table (**Control Panel -> Administrative Tools -> Services -> Flash Drive File Detection and Removal**)

Additional Options for FLASHDETECT.INI

[MAIN]

DriveScanFrequency=number

This option defines how often the system is checked for disks that are inserted. The value is in milliseconds. The default value is 1000msec (or 1 second). One second is pretty good, students can't really load up anything within this time. However some older machines may become CPU resource intensive, so making this value bigger may reduce CPU load.

[MAIN]

FileTimeOut=number

This option defines how often an attempt is made to write to a file on a shared network resource. The default value is 10 (10 times). In other words if it cannot write to a file and tries more than 10 times it then gives up. Setting this value to low and having a large or busy network or a network across a slow link may in fact mean your log file (if stored on the network) may never actually get written to. However on the other hand, setting this option too high will slow the efficiency of the detector/scanner right down and actually steal/hog the CPU. If you are having troubles with network log files, try increasing this number.

[MAIN]

ShowTrayIcon=number

This option defines whether or not that system tray icon is displayed in the bottom right hand corner of the system tray. The default value is 1, which is the equivalent of it being displayed. If this icon is hidden the user cannot see it but they can still see any configured actions. The only way an administrator can shut it down is to either stop

the service if it is configured in service mode or kill the process through task manager if configured in Interactive Application mode.

Now for some legal stuff

The standard edition (also known as the lite edition) of the Flash Detect program is licensed as freeware by FreeMEG Computing Services (incorporating FreeMEG software) <http://www.freemeg.com/>

The license allows you to use this unrestrictive throughout your company/school site. This does not give you the right to distribute the software to other sites. You may however link to the FreeMEG computing services site.

Basic Support is provided via email through the FreeMEG Software website, but the response time is at our discretion. That is if we choose to respond at all. If you would like additional support, this can be arranged through a paid support agreement with FreeMEG Computing Services.

There are certain limitations that exist to the Flash Detect software. If you want modifications to the software to be made then FreeMEG Software reserves the right to quote for that work to be done.

FreeMEG Software accepts no liability for the loss of data from any version of the Flash Detect Program, including upgrades and cross grades. FreeMEG Software accepts no responsibility for any loss of data or infrastructure on your site.

FreeMEG Software reserves the right to terminate free licensing without further notice. FreeMEG Software reserves the right to terminate anyone's license for the Flash Detect Software.

All intellectual property for the Flash Detect Software (unless otherwise acknowledged), remains in the ownership of FreeMEG Software and its founder Solomon Box.

Updates

Updates can always be found on our website:

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