

Enforcer's Task Definition Utility, Version 1.0, 2001

The Task Definition Utility is a means to easily define the necessary tasks for Enforcer to provide the protection you desire for your system. It will detect tasks as they are executed and allow you to save these to a file that can be imported into Enforcer's setup.

What is a task and how do I properly define one?

What the items on the dialog mean...

How to use the Task Definition Utility...

Some specific examples...

Example 1: Prohibiting the user from getting to some basic system settings.

Example 2: Only allowing the user access to access to specific applications.

Example 3: Limit internet access to only a few pre-approved sites using exact matching.

Example 4: Limit internet access to only a few pre-approved sites using partial matching.

Example 5: Prevent users from installing their own software.

What is a task and how do I properly define one?

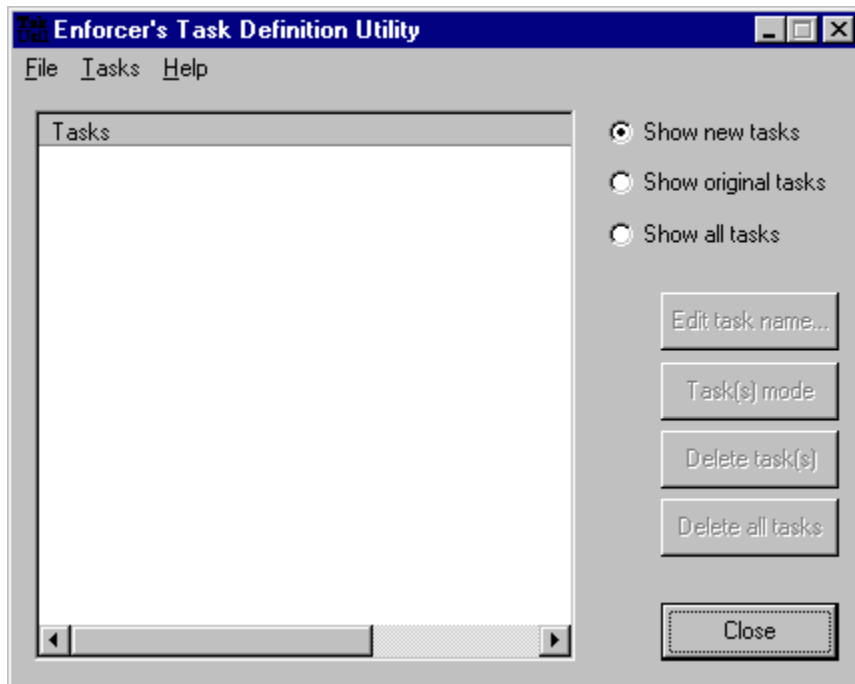
A task is how the operating system (Windows 95/98/Me or NT/2000) identifies active software components in the system. These components may be executables (programs) or applications, system dialogs or functions, or separate windows displayed by various programs. Usually, the task name of a program is the same as the text displayed in the title bar. The task name is not the same as the executable file name.

To properly protect some programs, partial task name matching must be used. For example, if you enter "Notepad" as the task name the software will protect "(Untitled) - Notepad" or "mytext.txt - Notepad". This is an example of task name matching at the end. If you enter "Exploring" as the task name, the software will protect Windows Explorer no matter what folder is chosen. This is an example of task name matching at the beginning. The software will not protect a task that has its name defined as a substring interior to the task name. For example, "Man" entered as a task name WILL NOT result in the protection of "File Manager".

The Task Definition Utility will allow you to provide the complete task name. If you need to edit a task name while in the Task Definition Utility, simply choose the task from the task list and press the Edit task name button.

What the items on the dialog mean

Working through a few simple examples will clarify how each of these items should be used to properly define tasks for Enforcer.



Dialog items

Tasks: This list contains the detected tasks that fall into the category specified by the radio buttons to the right of the list. The default is to display the new tasks. That is, the default is to display the tasks that are detected after the Task utility starts and not those tasks that are running when it starts. This is why the task list will be blank when the dialog first displays. Changing the radio button selection will change the contents of the task list.

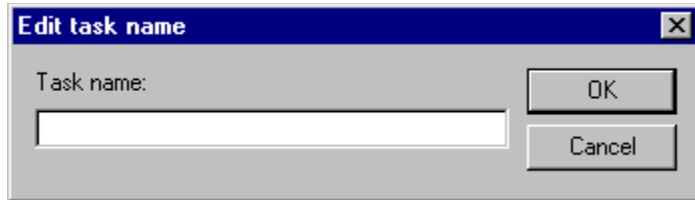
Each task in the task list will have an icon associated with it. If the icon is an "i", that specifies that Enforcer is to ignore this task and let it execute. If the icon is a circle with a slash through it, that specifies that Enforcer is to always prohibit that task from running.

Show new tasks: Selecting this option will display the tasks that started running after the Task Utility was executed. This option is the default and is the most useful option for defining tasks.

Show original tasks: Selecting this option will display the tasks that were already running when the Task Utility started.

Show all tasks: Selecting this option will display all of the tasks that the Task utility has detected, no matter when they were executed.

Edit task name: This button is enabled whenever a single task is selected in the task list. Selecting this button after a single task is selected will display a dialog that will allow you to edit the task name. This allows you to remove data specific information from the task name, such as a webpage name or a file name.



You may also use this function with the CTRL+E accelerator key or the Tasks->Edit task menu item.

Delete task(s): This button is enabled when one or more tasks are selected. Selecting this button will delete all the selected tasks. The default is to always confirm deletes, but this can be changed with the Tasks->Confirm task deletes menu item.

You may also use this function with the CTRL+D accelerator key or the Tasks->Delete task(s) menu item.

Task(s) mode: This button is enabled when one or more tasks are selected. Selecting this button will change the mode of all the selected tasks. This means that if a selected task's mode was ignore (the "i" icon), then changing its mode would change the icon to the circle with a slash through it. It would change from ignore mode, to prohibit mode.

Delete all tasks: This button is enabled when one or more tasks are displayed in the task list. Selecting this button will delete all tasks currently displayed in the task list.

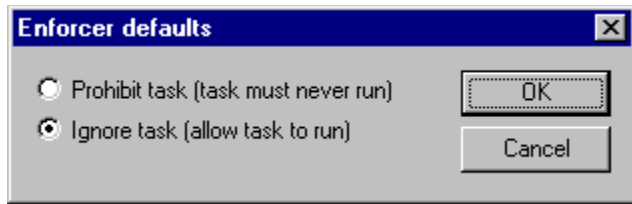
You may also use this function with the CTRL+C accelerator key or the Tasks->Delete all task(s) menu item.

Close: Selecting this button will close the task utility.

Menu items

File:

Set Enforcer defaults: This menu item will display the Enforcer defaults dialog



The default is for all detected tasks to be set to the ignore mode. This can be changed here so that any additional tasks that are detected are given the prohibit mode.

Save as Enforcer task file: This menu item will allow you to save the tasks currently displayed in the task list as an Enforcer task file. This task file can then be read into Enforcer's setup using the Import function.

Tasks:

The items in the task menu are the same as the buttons by the same name. These functions are detailed above.

How to use the Task Definition Utility

How you use the Task Definition utility will depend on how you wish to run Enforcer. There are basically two way to configure Enforcer: only prohibit specific tasks or only allow specific tasks. The two workflows are similar, but have a few key differences.

A hybrid workflow that uses elements of both of these workflows to limit internet access is provided in the Same specific examples section of this helpfile.

Here is the general workflow to only prohibit specific tasks.

- Run the Task Definition utility
 - Select the File->Set Enforcer defaults menu item. When the dialog displays, set the default to be Prohibit task. Dismiss the dialog with an OK.
 - Make sure that the Show new tasks radio button is selected on the main dialog.
 - Execute each task (program or system function such as Start->Run) that you wish to prohibit the user from using. As these tasks are executed, their task name will appear in the task list of the Task Definition Utility dialog. The icon associated with each task will be a circle with a slash through it. This designates these tasks as ones that should never be allowed to run.
 - When you have executed all the tasks that you wish to prohibit, select the File->Save as Enforcer task file menu item and save the tasks to a file.
-
- Run Enforcer's setup
 - Choose the File->Import menu item and open the file you have just saved.
 - Make sure the Options->Prohibit all tasks except those specified menu item IS NOT checked.
 - Set any other desired options and exit Enforcer's setup with the OK button.
 - Now, you are ready to run Enforcer!

Here is the general workflow to only allow specific tasks

- Run the Task Definition utility
 - Select the File->Set Enforcer defaults menu item. When the dialog displays, set the default to be Ignore task. Dismiss the dialog with an OK.
 - Make sure that the Show new tasks radio button is selected on the main dialog.
 - Execute each task (program or system function such as Start->Run) that you wish to allow the user to execute. As these tasks are executed, their task name will appear in the task list of the Task Definition Utility dialog. The icon associated with each task will be an "i". This designates these tasks as ones that should be allowed to run.
 - For each task that you wish to allow, work through the various functions and sub dialogs of the task, such as options dialogs, open dialogs, and so on. This will make sure that all the sub tasks of the main task are allowed to run also.
 - When you have executed all the tasks that you wish to allow, select the File->Save as Enforcer task file menu item and save the tasks to a file.
-
- Run Enforcer's setup
 - Choose the File->Import menu item and open the file you have just saved.

- Make sure the Options->Prohibit all tasks except those specified menu item IS checked.
- Set any other desired options and exit Enforcer's setup with the OK button.
- Now, you are ready to run Enforcer!

More specific examples are provided in the Some specific examples section of this helpfile.

Some specific examples

The resulting Enforcer task files for these examples can be found in the program directory.

The first example (example1.etk) shows how to prohibit specific programs and/or system functions while allowing all others to execute: Example 1.

The second example (example2.etk) shows how to only allow your users access to a specific set of programs and/or system functions while preventing everything else: Example 2.

A hybrid of the workflow combining elements from example 1 and 2 can be used to limit internet access to pre-approved webpages (such as on a VPN). Example #3 uses exact matching (iexplore3.etk and netscape3.etk) and example #4 uses partial matching (iexplore4.etk and netscape4.etk). For Netscape 6 users, use the example files netscape6_3.etk and netscape6_4.etk.

Another useful example (install.etk) is how to prevent users from installing their own software: Example 5.

Example 1: Prohibiting the user from getting to some basic system settings.

This example will demonstrate how to prohibit the user from getting to some basic system settings. We will use the Control Panel, Display Properties, Printers, and Taskbar Properties for this example.

- 1) Run the Task Definition Utility. The main dialog will appear with an empty list.
- 2) Select the “File->Set Enforcer defaults” menu item. When the dialog appears, change the setting to “Prohibit task”. This will indicate to the software that every task you add is a task you do not want the user to have access to. Dismiss the dialog with the OK button.
- 3) Display the Control Panel using “Start->Settings->Control Panel”. When the Control Panel is displayed, the task “Control Panel” will appear in the task list of the Task utility dialog. This task will have an icon associated with it that indicates that the task is prohibited.
- 4) Display the Display Properties dialog using the right mouse button menu from the desktop. When the Display properties dialog is displayed, the task “Display Properties” will appear in the task list of the Task utility dialog. This task will have an icon associated with it that indicates that the task is prohibited.
- 5) Using the “Start->Settings->Printers” and the “Start->Settings->Task & Start menu” entries on the Start menu, display the Printers and Taskbar Properties dialogs. The appropriate tasks will be added to the task list.
- 6) Use the “File->Save as Enforcer task file” menu entry on the Task Definition dialog to save your tasks to a file. You can then read these tasks into Enforcer’s setup, enfset.exe, to configure Enforcer. The file example1.etk contains the results for these steps.

This example’s purpose is to prohibit the user from using the four specified system functions. Here are the steps for reading this task file into Enforcer’s setup and configuring it to prohibit these four system functions, but allow anything else to run.

- 1) Run Enforcer’s setup, enfset.exe.
- 2) If there are any tasks displayed in the task list that you wish to keep, use the “File->Save as Enforcer task file” to save these to a file. This way you can always restore them later.
- 3) Use the “Tasks->Delete all tasks” menu item to clear the task list.
- 4) Use the “File->Open Enforcer task file” to open the file you saved in step 6 above. The tasks you defined using the Task Definition Utility will appear in the task list.
- 5) Make sure that the “Options->Prohibit all tasks except those specified” menu item IS NOT checked. This will indicate to the software that only the four tasks defined should be prohibited and anything else can run.
- 6) Define your password and any other settings you desire, then save the configuration with the OK on the main dialog.
- 7) Run Enforcer, enfrun.exe, and try it out.

Example 2: Only allowing the user access to access to specific applications.

This example will demonstrate how to only allow the user to access applications that you specify. This will, in effect, prohibit the user from doing anything except what you want the user to do. In this example, we will limit the user to a single game: Solitaire.

- 1) Run the Task Definition Utility. The main dialog will appear with an empty list.
- 2) Select the "File->Set Enforcer defaults" menu item. When the dialog appears, make sure the setting is set to "Ignore task". This will indicate to the software that every task you add is a task you want the user to have access to. Dismiss the dialog with the OK button.
- 3) Run Solitaire. This is a card game delivered with Windows and can be found under the Start menu. When Solitaire is displayed, the task "Solitaire" will appear in the task list of the Task utility dialog. This task will have an icon associated with it that indicates that the task is to be ignored. This means that Enforcer will allow this task to run.
- 4) We want the user to be able to use any sub-tasks used by Solitaire, so we need to exercise the software a bit to make sure these sub-tasks are captured by the Task Definition Utility. Select the "Help->About" menu item. This will display the About box for Solitaire and the associated task will be shown on the Task Definition Utility main dialog.
- 5) Select the "Game->Deck" and the "Game->Options" menu items. These tasks will also be added. Also, select the remaining menu items on Solitaire's Help menu. By adding the tasks in this step and step 4, you tell the software to allow Solitaire and its various function to run.
- 6) Use the "File->Save as Enforcer task file" menu entry on the Task Definition dialog to save your tasks to a file. You can then read these tasks into Enforcer's setup, enfset.exe, to configure Enforcer. The file example2.etk contains the results for these steps, plus step 6 below.

This example's purpose is to only allow the user to run one application: Solitaire. Here are the steps for reading this task file into Enforcer's setup and configuring it to only allow this one application, while prohibiting everything else..

- 1) Run Enforcer's setup, enfset.exe.
- 2) If there are any tasks displayed in the task list that you wish to keep, use the "File->Save as Enforcer task file" to save these to a file. This way you can always restore them later.
- 3) Use the "Tasks->Delete all tasks" menu item to clear the task list.
- 4) Use the "File->Open Enforcer task file" to open the file you saved in step 6 above. The tasks you defined using the Task Definition Utility will appear in the task list.
- 5) Make sure that the "Options->Prohibit all tasks except those specified" menu item IS checked. This will indicate to the software that you only want to allow the tasks that are shown in the Task list. Anything else should not be allowed to run.
- 6) Some tasks used by Windows must be directly specified to never run. These tasks are "Display Properties", "Taskbar Properties", and "Run" (no quotes, of course). You must add these tasks manually using the Add Task button on the main dialog. Make sure these tasks are defined as "Prohibit task".
- 7) Define your password and any other settings you desire, then save the configuration with the OK on the main dialog.
- 8) Make sure that you exit any applications you do not want Enforcer to close for you and then run Enforcer, enfrun.exe, and try it out.

Example 3: Limit internet access to only a few pre-approved sites using exact matching.

This example will demonstrate how to limit the user to a few selected webpages that you specify and still use anything else on the system. This will, in effect, prohibit the user from going anywhere on the internet, except where you want the user to go. In this example, we will limit the user to two webpages on our website, <http://posum.com>, using exact matching. An example of using partial matching to allow all the webpages on our website, but no other webpages, is available through this link. Partial matching works well if the allowable webpage titles are similar, such as they sometimes are on an intranet or VPN. We will use Microsoft Internet Explorer (iexplore3.etk) for this example, but a task file for Netscape, netscape3.etk, is also provided. For Netscape 6 users, use the example file netscape6_3.etk.

- 1) Set <http://posum.com/index.html> to be your home page in Internet Explorer. Do this through the Tools->Internet Options menu item on the General tab.
- 2) Run the Task Definition Utility. The main dialog will appear with an empty list.
- 3) Select the "File->Set Enforcer defaults" menu item. When the dialog appears, make sure the setting is set to "Ignore task". This will indicate to the software that every task you add is a task you want the software to ignore. That is, for user to have access to. Dismiss the dialog with the OK button.
- 4) Run Internet Explorer. Posum's home page should appear. Two tasks should appear in the Task Definition Utilities task list. One task should have the actual web address of the webpage and the other a more descriptive title. If you do not have two tasks, press Refresh a few times. These tasks will have an icon associated with them that indicate that the tasks are to be ignored. This means that Enforcer will allow these tasks to run.
- 5) Select the graphic on the left of the webpage that says Windows Enforcer. This will take you to Enforcer's webpage. Two tasks should appear in the Task Definition Utilities task list. One task should have the actual web address of the webpage and the other a more descriptive title. If you do not have two tasks, press Refresh a few times. These tasks will have an icon associated with them that indicate that the tasks are to be ignored. This means that Enforcer will allow these tasks to run.
- 6) Use the "File->Save as Enforcer task file" menu entry on the Task Definition dialog to save your tasks to a file. You can then read these tasks into Enforcer's setup, enfset.exe, to configure Enforcer. The file iexplore3.etk contains the results for these steps, plus step 8 below. A netscape file is also available, netscape3.etk.

So far, this example's purpose is to only allow the user to visit two webpages that you specify. If the name of the allowable webpages are similar (such as an intranet or VPN sometimes are), you can use partial matching to make this easier. An example of modifying this example to allow all the webpages on our website is available through this link. Here are the steps for reading this task file into Enforcer's setup and configuring it to restrict the user to the specified webpages, but allow anything else to run.

- 1) Run Enforcer's setup, enfset.exe.
- 2) If there are any tasks displayed in the task list that you wish to keep, use the "File->Save as Enforcer task file" to save these to a file. This way you can always restore them later.
- 3) Use the "Tasks->Delete all tasks" menu item to clear the task list.

- 4) Use the “File->Open Enforcer task file” to open the file you saved in step 6 above. The tasks you defined using the Task Definition Utility will appear in the task list.
- 5) Make sure that the “Options->Prohibit all tasks except those specified” menu item IS NOT checked.
- 6) Now we must manually define a task to prohibit all the websites except those we have defined. While Internet Explorer is still running, press the Add Task button.
- 7) When the Add Task dialog appears, select the Browse button to the right of the Task name field and select the task associated with Internet Explorer.
- 8) Once you return to the Add Task dialog, edit the task name to be “ – Microsoft Internet Explorer” (no quotes of course). Make sure that the option at the top of the Add Task dialog is set to “Prohibit task” and then choose OK on the Add Task dialog. This task will prohibit any webpage, except the ones you have specified that Enforcer should ignore.
- 9) Define your password and any other settings you desire, then save the configuration with the OK on the main dialog.
- 10) Run Enforcer, enfrun.exe, and try it out.

NOTE: If you experience unexpected behavior when trying this example, cut on the logging feature to see what tasks Enforcer is terminating. One common problem is the definition of the home page. It is possible to get “<http://posum.com/> - Microsoft Internet Explorer” as the task name for the home page in some cases instead of “<http://posum.com/index.html> - Microsoft Internet Explorer” as defined in this example. If you get the one without index.html, just add the new task as one to be ignored and continue. Here is an example of cutting on the log file.

- 1) Run Enforcer setup, enfset.exe, and select the “File->Log file” menu item.
- 2) Make sure the “Log activity to file” check box is checked and the “Append to file” check box is not checked. This will only save the logfile information during one run of Enforcer, enfrun.exe.
- 3) Set the Log file field to the desired file name. An example is “C:\temp\test.log”.
- 4) Set the time and date functions as you prefer, and dismiss the dialog with the OK button.

Example 5: Prevent users from installing their own software.

This example really does not need the Task Definition Utility, but it is included here since it is a useful example.

Preventing users from installing their own software is a fairly simple process. Here are the steps. The resulting task file is install.etk and is available in the program directory.

- 1) Run Enforcer setup, enfset.exe.
- 2) Save the tasks you currently have defined to a file and then delete all the tasks in your task list. The “Tasks->Delete all tasks” menu item makes this easy.
- 3) Use the “File->Open Enforcer task file” menu item to read in the file install.etk.
- 4) You will see a collection of tasks that are variations on the word install and setup. All but one of these tasks has an icon associated with it that is a circle with a slash through it. These tasks make sure no software is installed on the system.
- 5) The task “Page Setup” has an icon with an “i” associated with it. This indicates to the software that Enforcer should ignore or allow this task to run. This task is included so Enforcer will prevent a user from installing his own software, but it will allow the user to use the “Page Setup” command in Microsoft Word. This task demonstrates how to specify an exception. That is, this task indicates that “Page Setup” should be allowed to run even though it matches a prohibited task “Setup”.
- 6) Make sure the “Options->Prohibit all tasks except those specified” IS NOT checked.
- 7) Save with an OK.

Now you are ready to run Enforcer, enfrun.exe, and try it out.

Example 4: Limit internet access to only a few pre-approved sites using partial matching.

This example will demonstrate how to only allow the user to access a few selected webpages that you specify and still use anything else on the system. This will, in effect, prohibit the user from going anywhere on the internet, except where you want the user to go. In this example, we will limit the user to only the webpages on our website, <http://posum.com>. This example uses partial task matching and is useful if the allowable webpages have similar titles, such as they sometimes do on an intranet or VPN. If the webpage titles are different, then exact matching will be required. An example of exact matching is available through this link. We will use Microsoft Internet Explorer for this example, but a task file for Netscape, `netscape4.etk`, is also provided. For Netscape 6 users, use the example file `netscape6_4.etk`.

- 1) Set `http://posum.com/index.html` to be your home page in Internet Explorer. Do this through the “Tools->Internet Options” menu item on the General tab.
- 2) Run the Task Definition Utility. The main dialog will appear with an empty list.
- 3) Select the “File->Set Enforcer defaults” menu item. When the dialog appears, make sure the setting is set to “Ignore task”. This will indicate to the software that every task you add is a task you want the software to ignore. That is, for user to have access to. Dismiss the dialog with the OK button.
- 4) Run Internet Explorer. Posum’s home page should appear. Two tasks should appear in the Task Definition Utilities task list. One task should have the actual web address of the webpage and the other a more descriptive title. If you do not have two tasks, press Refresh a few times. These tasks will have an icon associated with them that indicate that the tasks are to be ignored. This means that Enforcer will allow these tasks to run.
- 5) Use the “File->Save as Enforcer task file” menu entry on the Task Definition dialog to save your tasks to a file. You can then read these tasks into Enforcer’s setup, `enfset.exe`, to configure Enforcer. The file `ieexplore4.etk` contains the results for these steps, plus the steps below. A netscape file is also available, `netscape4.etk`.

Partial matching can be used to allow all the webpages on our site because the webpage titles are all similar. Every webpage on our site begins with the text “Posum.com –“. Also, all the web addresses for our webpages start with “<http://posum.com>”. This allows us to define two tasks to allow all of the webpages at our website. Here are the steps for reading this task file into Enforcer’s setup and configuring it to restrict the user to the webpages on our website using partial matching, but allowing anything else to run.

- 1) Run Enforcer’s setup, `enfset.exe`.
- 2) If there are any tasks displayed in the task list that you wish to keep, use the “File->Save as Enforcer task file” to save these to a file. This way you can always restore them later.
- 3) Use the “Tasks->Delete all tasks” menu item to clear the task list.
- 4) Use the “File->Open Enforcer task file” to open the file you saved in step 5 above. The tasks you defined using the Task Definition Utility will appear in the task list.
- 5) Make sure that the “Options->Prohibit all tasks except those specified” menu item IS NOT checked.
- 6) Now we must manually add a task to prohibit all webpages except those we have defined as exceptions. While Internet Explorer is still running, press the Add Task button.

- 7) When the Add Task dialog appears, select the Browse button to the right of the Task name field and select the task associated with Internet Explorer.
- 8) Once you return to the Add Task dialog, edit the task name to be “ – Microsoft Internet Explorer” (no quotes of course). Make sure that the option at the top of the Add Task dialog is set to “Prohibit task” and then choose OK on the Add Task dialog. This task will prohibit any webpage, except the ones you have specified that Enforcer should ignore.
- 9) Now, we need to modify the two tasks that define the webpages we wish to allow. Select the task that begins with the text “Posum.com –“ and press the Edit task button. When the Edit task dialog appears, modify the task name to be “Posum.com –“ (no quotes of course...) and press OK on the Edit task dialog.
- 10) Select the task that begins with the text “http://posum.com” and press the Edit task button. When the Edit task dialog appears, modify the task name to be “http://posum.com“ (no quotes of course...) and press OK on the Edit task dialog.
- 11) Define your password and any other settings you desire, then save the configuration with the OK on the main dialog.
- 12) Run Enforcer, enfrun.exe, and try it out.

NOTE: If you get unexpected behavior when trying this example, cut on the logging feature to see what tasks Enforcer is terminating. Here is an example of cutting on the log file.

- 1) Run Enforcer setup, enfset.exe, and select the File->Log file menu item.
- 2) Make sure the Log activity to file check box is checked and the Append to file check box is not checked. This will only save the logfile information during one run of Enforcer, enfrun.exe.
- 3) Set the Log file field to the desired file name. An example is “C:\temp\test.log”.
- 4) Set the time and date functions as you prefer, and dismiss the dialog with the OK button.

